**Arizona GEAR UP Policies and Procedures for Data Security and for Safeguarding Personally Identifiable Information**

**Overview of the Data Security Policy**

All personally identifiable data collected by Arizona GEAR UP will be maintained in a secure manner. The key components of the data security plan are provided below. Additional details regarding the safeguarding of Personally Identifiable Information (PII) are described in the remainder of this document.

1. Arizona GEAR UP personnel involved in data management/analysis will be FERPA trained and will have gone through an appropriate level of background check.
2. The Arizona GEAR UP database will be password protected and access to this database will be controlled based on the access required by Arizona GEAR UP personnel to complete grant-related duties.
3. A third party vendor charged with creating and maintaining the Arizona GEAR UP database will provide written documents detailing their security policies and evidence that their database meets industry data security standards.
4. Arizona GEAR UP staff will ensure that electronic and paper copies of downloaded data will be maintained in locked cabinets within a locked office while not in use.
5. Exchanges of data between GEAR UP School District Partners and Arizona GEAR UP will be done according to the security requirements of the participating GEAR UP partners.
6. Per requirements established by the federal government and Northern Arizona University, data provided by GEAR UP School District Partners will be destroyed five years from the conclusion date of this project.

**Safeguarding Personally Identifiable Information (PII)**

Employees of Arizona GEAR UP that have access to student-level data are responsible for safeguarding PII contained within those data. PII is defined as information that can be used to identify, contact, or locate individual students, educators, or their families, or that can be combined together with other information to deduce the identities of individual students, educators, or families. Examples of PII that are maintained by Arizona GEAR UP include the following.

* Students’ Full Name
* Home Address
* Phone Number(s)
* Date of Birth

Examples of information within the Arizona GEAR UP database that potentially can be combined with other information to personally identify GEAR UP students include:

* Country, state, or city of residence
* [Gender](http://en.wikipedia.org/wiki/Gender) or race
* Name of the school they attend

Arizona GEAR UP recognizes that there are both authorized and unauthorized disclosures of PII. An Authorized Disclosure is a disclosure of PII to:

1. Arizona GEAR UP employees who need access to PII in order to complete their assigned data entry or analysis activities.
2. A third party that is contracted to maintain the Arizona GEAR UP database. This third party is contractually obligated to protect PII.
3. Other government agencies for legally required or authorized purposes;
4. Individual students and their parents (depending on the age of the student) for whom the PII is recorded.

In any of these cases, disclosure of PII requires the approval of the appropriate Arizona GEAR UP supervisor.

In safeguarding PII, it is important to remember that there can be unauthorized disclosures of PII that occur both within Arizona GEAR UP and between Arizona GEAR UP and other agencies and persons. Within Arizona GEAR UP, an unauthorized disclosure occurs when PII is revealed to an employee of Arizona GEAR UP that does not have a legitimate need to know that information. For example, this could occur if documents with PII are left unattended on copy machines, or if PII from one GEAR UP Partner is shared with a second GEAR UP Partner without permission. An unauthorized disclosure with outside agencies or persons occurs when data with PII are shared with individuals outside of GEAR UP that are **not** authorized to have that information. For example, PII is inadvertently revealed as part of an evaluation or research report.

**Risk prevention.** Given the potential serious consequences to Arizona GEAR UP and to its individual employees, it is important to work with PII in such a way as to reduce and hopefully eliminate the possibility of an inappropriate disclosure of PII. Here are some guidelines for Arizona GEAR UP in this regard.

1. Do not identify individual students by name or ID in any reports of findings.
2. Always limit the amount of PII in any downloaded or created work file to the minimum amount of PII necessary.
3. Follow best practice suggestions for reporting disaggregated subgroup data in order to protect students’ identities.

(See <http://nces.ed.gov/pubs2011/2011603.pdf>.)

1. When possible, use receipt-required mail delivery systems or encrypted electronic files to exchange data. Always verify the recipient’s address before sending or requesting data.
2. Do not leave a computer with accessible PII unintended in a non-password protected mode. Turn off computers at the end of the business day.
3. Place hard and electronic copies of data with PII in locked file drawers before leaving at the end of the day.
4. Ensure that computers that have contained PII are erased before turning them in or disposing of them.
5. Computer passwords should be kept confidential and changed periodically.
6. Notify IT if spyware or other viruses are detected that could compromise PII. The IT representative and the Arizona GEAR UP supervisor should cooperate in assessing the level of risk.

**Reporting an unauthorized disclosure of PII.** All unauthorized disclosures of PII must be reported to the employee’s supervisor immediately. This applies to both known and suspected disclosures. The initial report can be done by speaking with the supervisor, but it should be followed up as soon as possible by a written report with the following details.

 Your name

 Date/approximate time that unauthorized disclosure was detected

 Nature of the suspected or known unauthorized disclosure

 The PII data that was lost or compromised

 Steps taken if any to recover the PII/

Other relevant information

Once notified, the supervisor will work with the employee to assess the level of risk associated with the unauthorized disclosure and to take the necessary steps to notify concerned parties about the disclosure, retrieve/protect the data if possible, and to prevent further unintended disclosures of PII.