Best Practices for Handling UINs

i-card Programs Help Desk ● (217) 265-6464 ● icardhelp@uillinois.edu

The following practices have been approved as acceptable ways to handle University identification numbers (UINs) in daily operations. They are based on the University's UIN policy (www.obfs.uillinois.edu/manual/central_p/sec19-3.html).

The i-card Programs Office can help offices to adopt new practices to comply with these guidelines. If your office would like such assistance, please contact i-card Programs' Help Desk.

Use UINs for unique identification. UINs are intended to identify a specific individual without confusing that person with someone else who has the same or a similar name. UINs were created so that the University would not have to use Social Security numbers for this purpose. UINs should therefore be used any time you need to uniquely identify a person, such as when you are looking up their records or data.

Do not use UINs as passwords or to prove that someone is who he or she claims to be. Most UINs are not confidential, so a person's UIN may be known to other people. Therefore, UINs must never be used to verify that a person is who she or he claims to be (that is, for authentication). UINs must never be used as passwords, whether verbally or electronically, in person, or over the phone. UINs must not be used in part or in full for posting grades or any other nonpublic information.

Share UINs freely with other University personnel when conducting University business. Offices across the University need to be able to uniquely identify students, faculty, staff, and others in their day-to-day work. UINs are intended to enable that work and may be freely shared among University personnel on University systems in order to conduct University business.

Avoid sharing UINs off campus or with non-University personnel. UINs are intended to facilitate University business and are not meant for off-campus use. In most cases, it is not illegal to share UINs off campus, but there are some cases where it is (see the next three topics for details). In addition, campus FERPA policies ban public display or general publication of UINs. Because of these restrictions, it is best not to share UINs off campus, unless the sharing takes place under a University contract with appropriate confidentiality language in place. If your office has a business need to share UINs with an outside party, contact the i-card Programs' Help Desk at (217) 265-6464 or icardhelp@uillinois.edu for the appropriate procedures.

If someone who is not a University employee asks you to tell them a UIN over the phone, refer them to i-card Programs' Help Desk, where procedures are in place to appropriately provide the information.

Student UINs are protected by the Family Educational Rights and Privacy Act (FERPA), even after a student graduates. Student UINs are classified as directory information

under FERPA. Student UINs should be handled in the same way as student addresses, phone numbers, and other directory information. FERPA protection remains in place even after a student graduates or leaves the University. Many faculty and staff members, visitors, and others with UINs are former or current students of the University of Illinois. Insofar as their UINs are used as student identifiers, FERPA protection applies. Contact your campus Registrar for further information on handling FERPA-protected data or to discuss FERPA-related cases:

> Chicago Campus Registrar — (312) 413-1878
>
> Springfield Campus Registrar — (217) 206-6174 or registrar@uis.edu
>
> Urbana Campus Registrar — (217) 333-0210 or registrar@illinois.edu

Some student UINs are confidential and must be treated securely. Students may opt to suppress their FERPA directory information. UINs for students who have done so are considered confidential under the law and must be treated securely, in line with the University's Information Security Policy (www.obfs.uillinois.edu/manual/central_p/sec19-5.html). A few practices to keep in mind are:

- Whenever UINs are emailed, there is a risk of the email being forwarded to systems outside of the University's secure systems. If you are handling FERPA-suppressed UINs, consider using the phone, PEAR (www.obfs.uillinois.edu/jobaids/ JA_PEAR.pdf), or NetFiles (www.cites.illinois.edu/netfiles/) as alternatives.

- Do not store suppressed UINs on your desktop computer unless you can encrypt the files containing them. Instead, use secure University servers to store them.

- Do not store suppressed UINs on mobile devices such as laptops, CDs, or flash drives.

- Store paper records containing suppressed UINs securely and dispose of them securely (for instance, by shredding).

- If a FERPA-suppressed UIN is released in an unauthorized manner at any time, regardless of what other data is released, the responsible unit should phone (not email) i-card Programs' Help Desk at (217) 265-6464 to determine the proper course of action.

Confidential UINs remain so permanently. Confidential status remains in place even after a student leaves the University. For faculty and staff members, visitors, and others who are former or current students, confidential status applies to the UIN insofar as it is used as a student identifier. Contact your campus Registrar for more information or to discuss FERPA-related cases.

Do not use UINs in logins. Many members of the University community have access to more than one electronic system and may have separate logins for each one. The i-card Programs Office supports the University's efforts to minimize the number of logins each person needs. Therefore, the OBFS UIN policy bans the use of UINs as any part of a login. Enterprise IDs and NetIDs are widely used alternatives, and i-card Programs encourages their use. If there is a reason that your unit cannot use Enterprise IDs or NetIDs for logins, contact i-card Programs' Help Desk at (217) 265-6464 or icardhelp@uillinois.edu to determine whether an exception can be made.