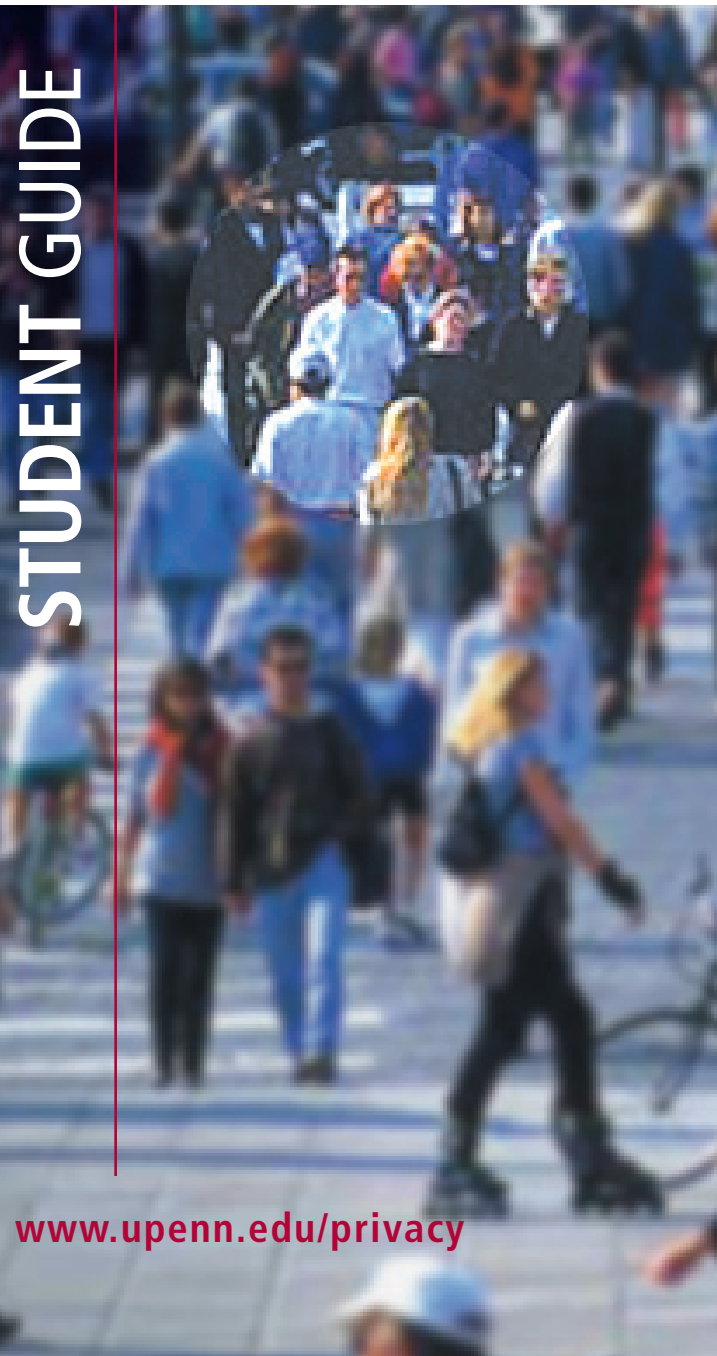




The smartest way to protect your privacy is to be aware of the types of privacy issues that exist, the choices you have, and to make decisions that are right for you.



STUDENT GUIDE



www.upenn.edu/privacy

YOUR RIGHTS AND CHOICES

The Federal Educational Rights and Privacy Act (FERPA) provides students a number of privacy rights for student records.

RIGHT TO CONSENT TO SHARING STUDENT RECORDS – GRADES, FINANCIAL, AND MORE

Students have the right to consent to the disclosure of information contained in their education records, except to the extent that FERPA authorizes disclosure without consent. The most significant exception to the consent requirement allows sharing with school officials with a “legitimate educational interest” – in other words, where the information is required or would be helpful in the performance of his or her duties, or in the pursuit of an enterprise sanctioned by the University. Also, Penn may share student records with other colleges or universities to which a student is applying.

At Penn, you can consent to the disclosure of your student education records online. To do so, visit the Penn Portal, and use the “Online Consent Form” under “My Privacy Settings”. For a paper version of the consent form, visit Penn’s Privacy website.

ABOUT DIRECTORY / CONTACT INFORMATION

By law, Penn may release your “directory information” without your consent, unless you have specifically asked Penn not to do so (“opted out”). At Penn, “directory information” may include your local and home address, e-mail, telephone number, birthdate, major, degrees, awards, activities, etc. (See Penn Privacy website for complete list.)

Penn’s online directory protects you beyond the legal requirement and allows you to opt-out of sharing most types of directory information in two ways – within the Penn community and with the general public. To do so, visit the Penn Portal and click on “Directory Information” under “My Privacy Settings”. For more information and options, contact the Office of the Registrar.

RIGHT TO REVIEW RECORDS

To exercise your right to review your student records, send a written request to the official responsible for the records. Contact your School office if you have questions about who that is. Penn will make records subject to review available within 45 days.

RIGHT TO SEEK CORRECTION OF RECORDS

You also have the right to seek correction of your records. Again, submit in writing the information you wish to have corrected and the reason why to the responsible official. If your request is denied, Penn will notify you of the decision and advise you of the right to a hearing.

RIGHT TO FILE COMPLAINT WITH DEPARTMENT OF EDUCATION

Students have the right to file a complaint with the U.S. Department of Education concerning alleged noncompliance with FERPA by writing to:

The Family Policy Compliance Office
U.S. Department of Education
400 Maryland Ave. SW
Washington, D.C. 20202-4605

YOUR LIFE ONLINE

ONLINE NETWORKING SERVICES

Many online services offer students terrific ways to develop social and professional networking opportunities. But, think about how much you want to share and with whom.

Remember that once you post data about yourself, it may be very hard to take it back. Do you want to let the world know your physical address or your summer plans? Maybe you're comfortable sharing only your e-mail address and only with a designated known group of people. Click on privacy links on these online services websites (such as Facebook.com) and make smart choices about what you share and with whom.

DISCUSSION BOARDS, BLOGS, WEB POSTINGS

Think about privacy risks also when posting to discussion boards, blogs, and other websites. Posts made on the web may well be permanent and may define the writer now or at any future point. Statements made now, in jest or between what the writer assumes to be a small group of friends, may come back to haunt in the future. Consider who may conduct a web search of your name in the future – including potential employers – and what they may find. Think before you speak – and type!

BEWARE OF "PHISHING" SCAMS

"Phishing" attacks usually take the form of a spoofed e-mail, pretending to be from a bank, retailer, or other legitimate institution, and usually request the reader to urgently provide account information, passwords, social security numbers and other sensitive data. Some of these e-mails may also try to plant software such as keylogger programs to gather your data.

Do not respond to any e-mail with a request for personal information such as passwords, social security numbers, credit card numbers, account numbers and other sensitive data. And do not click on any links, or open any attachments, from a message that you think may not be legitimate.

SPAM FILTERING SERVICES

Unsolicited commercial e-mail, commonly referred to as "spam," has risen exponentially in recent years and now accounts for 40-65% of all e-mail traffic. Spam is a problem for anyone with an email account. Spam messages themselves can be quite annoying or offensive. The messages can include attachments and URLs that, if clicked on, can install viruses on your computer. Also, spam uses up your e-mail quota and the amount of spam may overwhelm legitimate e-mail, making legitimate e-mail harder to locate.

Many e-mail servers on campus offer a spam filtering service. To learn more about these services, visit Penn's Privacy website.



YOUR LIFE OFFLINE

MARKETING OFFERS

The world of marketing has changed dramatically in recent years. Through advancements in technology and law, consumers have new opportunities to receive marketing communications and to stop them as well. Students concerned about privacy should consider some prominent programs to stop certain communications and in some cases to reduce the risk of ID theft.

- National Do Not Call Registry – If you wish to stop receiving most telemarketing calls, visit <http://www.donotcall.gov> or call 1-888-382-1222.
- Pre-Approved Credit Offers – These offers can be abused by identity thieves who go through trash cans (sometimes called "dumpster divers") and open up credit in your name. If you wish to stop receiving these offers, call 1-888-5-OPTOUT.
- Direct Marketing Association's Mail Privacy Program – To receive less commercial advertising mail, you can register for The DMA's Mail Preference Service (MPS).
- Look for additional privacy options at the Penn Privacy website.

BE STREET SMART WITH YOUR PERSONAL DATA

Online or off, it's important to think about how valuable your data is and how best to protect it. Be aware of the distance and behavior of others when you're inputting PINs at ATM machines or passwords elsewhere. Consider special safety issues in providing your physical address; spam issues in providing your e-mail address; and telemarketing concerns in providing your phone number. In general, look for opportunities to exercise control over and to secure your data and make choices that are right for you.

YOUR IDENTITY

CREDIT REPORTS – YOUR FINANCIAL IDENTITY

You probably already know that it's important to pay your bills on time, to avoid late fees and other penalties. But do you also know that when you do not pay your bills on time, that "late" status is probably recorded by one of three credit reporting agencies in a credit report about you? And, these agencies have the right to share such information with others when you apply for credit, insurance, or jobs (in the case of jobs, with your consent) in the future.

It is a smart idea to review the information that credit reporting agencies collect about you to make sure that they have your information right and to determine if perhaps an imposter has taken out credit in your name (a popular form of identity theft). You are entitled by law to one free credit report a year from each agency. See <http://www.annualcreditreport.com>.

MINIMIZE YOUR RISK OF IDENTITY THEFT

Identity theft is a crime that occurs when a thief uses someone's personal information to commit fraud or theft. Typically, an identity thief uses another's personal information to open a credit account in the victim's name, or takes over an existing account and runs up fraudulent charges. The victims may not find out about the theft until they realize that their credit reports show unpaid balances. This could threaten their ability to secure a loan, a mortgage – even a job!

While you cannot completely protect yourself against identity theft, you can take steps to minimize your risk. Below are suggestions, including many from the Federal Trade Commission, for minimizing such ID theft risk:

- Do not give out personal information unless you've initiated the contact or are sure you know who you're dealing with.
- Guard your mail and trash from theft. Tear or shred documents containing your personal information.
- Place hard-to-guess passwords on your credit card, bank, and phone accounts where possible.
- Secure personal information in your home.
- Don't carry documents that contain your personal information, such as your social security number, unless absolutely necessary!
- Secure your computer with anti-virus software, strong passwords, promptly applied security patches, and a firewall.

For more information on identity theft, including how to tell if you've been victimized and/or what to do if you are a victim, visit <http://www.consumer.gov/idtheft>. And, if you believe you are a victim of identity theft, please contact the Penn Police at 215-898-4485.

www.upenn.edu/privacy