Web sites can be “archived” or “cached” so people can still access the old content even if the Web site disappears or changes. This means that any information posted to the Web could be online for a long time - maybe even forever. Internet Archive (www.archive.org) has 55 billion Web pages!

**Blogs & Social Networking**

Have you put your profile on a social networking site like MySpace or Facebook, an online dating or alumni site? Have you set your profile to be private? If not, anyone who visits that site, including college admissions offices, teachers, family, potential employers or even stalkers can see your personal information.

Do you use free e-mail, a blog, instant messaging, or share music or photos online? When you signed up for that service, did you give your name, age, gender, the town you live in or your hobbies? If so, the company that got your information might post it online for everyone to see. Many times, you can choose not to have your information included in public directories. You can also provide very little information if you want (only your first name or a fake name, for example).

Have you ever played in the school band, had your work included in an art show, or been on a sports team? If so, your name, personal details, and contact information might be posted online. Some Web sites will remove information at your request, but if the site is archived, your information may not really be gone. If you don't want information posted online, you should act quickly to have it removed.

**Archives**

Web sites can be “archived” or “cached” so people can still access the old content even if the Web site disappears or changes. This means that any information posted to the Web could be online for a long time - maybe even forever. Internet Archive (www.archive.org) has 55 billion Web pages!

**Other ways your information gets on the Web:**

- A store asks for your phone number or zip code when you buy something and that information is put into a database. The store might later sell your information to a data broker who posts it in an online directory.
- A friend or classmate posts information or photos that include you. Or, a relative posts a family photo album with you in it.
- If you have a drivers license, have gotten a traffic ticket or gone to Court, your name, address, and other personal information may be available online on a court or county Web site.

**Removing Information**

Sometimes it's okay to leave certain information online, especially if it's harmless. When trying to remove your information from any Web site, consider not sharing your correct information because data brokers make money by selling accurate information. If you want something removed, the Web site may have instructions, or provide a form or E-mail address to contact them. If the information is in a government record, you may need to fill out an official petition, motion, request or letter.

**How do I know what is on the Web already?**

- Search the Web for your personal information and photos. Some places to start: Google, Yahoo, Classmates.com, YouTube and Flickr.
- Look on Web sites for groups and places where you might have a connection: your school, clubs, jobs, faith community, sports teams, community and volunteer groups, etc.

Love is respected®

[LoveIsRespect](http://www.loveisrespect.org) - 11k

Cached: Sim
If you think there may be spyware on your computer try to use a safer computer when you look for help. It may be safest to use a computer at a library, friend’s house, community center, or Internet café.

• If you suspect that someone has the password to any of your accounts, go to a computer that this person doesn’t have access to and change your password. Only check that account from a computer that this person cannot access. The most secure passwords are at least 8 characters long and use a combination of letters and numbers.

• If you suspect that an abuser can access your E-mail or Instant Messages (IM), consider creating additional E-mail/IM accounts on a safer computer. Do not create or check new E-mail/IM accounts from a computer that might be monitored. Look for free Web-based E-mail accounts, and consider using non-identifying name and account information (example: bluecat@email.com and not YourReal-Name@email.com). Also, carefully read the registration screens so you can choose not to be listed in any online directories.

• Remember that many phones are just mini-computers. Stalkers can put spyware programs on cell phones and other handheld devices to track every text message sent and phone number dialed. Also, if someone knows or can guess your password, that person can log on to your phone account, bank account or other accounts online. So keep your passwords secret and change them often!