Confidentiality and Anonymity on the Web

Anonymity is maintained by the fact that it is not necessary for a school to use a tracking system to administer the survey. All students can login using the same user ID. These respondents are truly anonymous. Incentive tracking or follow up can be accomplished by the use of a separate self-declaration: a) post card or email stating their name and that they have completed the survey; or b) pop-up page at end of survey with a link to email or website where they can declare they completed the survey.

If a school wants to track the individual users this is also possible. The user is given a nine digit user ID. The user ID is the only information loaded onto the server. The student's name is not on the server, nor with their data. When the student enters data the user ID is not linked to the data. When the student's data is downloaded the user ID is not included with the download. The data that is archived is at that point anonymous.

The server maintains a single identifier for the data. The identifier is the password it assigns to the student upon initial login. This identifier is known only by the student and stays that way thanks to 2048-bit SSL encryption. The identifier serves as a locator for the data. It is not linked to the user nor downloaded with the data, thus keeping the data anonymous. It simply specifies the location of the data on the server in the event the student needs to stop and complete the survey later.

Confidentiality prior to download is protected as follows:

- When a respondent logs in for the first time, the server automatically generates and assigns them a password. Without the password no one can view their responses.
- The password is known only by the student and the server. The Core Institute does not know or have access to the user passwords.
- Once the student completes the survey the server locks that survey. The correct user ID with password will no longer grant access to the survey. This protects respondents from other household members who might find the user ID and password.
- The server is a dedicated server and not used for other purposes. It is not part of a larger network where staff outside the Core Institute might obtain access to it.
- The server is independently located behind firewalls. There is a firewall between the server and the public, and another firewall between the server and the Core Institute's network. The Core Institute's own network and archived data are also protected by this firewall. Other domains cannot access the server through the Core's network.

IP Addresses

For confidentiality the IP addresses are excluded from the transaction logs. No record of a student's visit is maintained on the server.

For security reasons most servers will not allow you to log on unless the other server has identified itself in some way. Our firewall will not allow an anonymous machine into the server as a means of protecting the data from potential attacks. If students are accessing through a LAN or Internet provider it is most likely that the outgoing IP's are dynamically linked, meaning that they are not directly associated with an individual machine. Instead the server uses an IP that is within a range of IP addresses reserved for outside connections. This is fairly standard practice as it protects the server from the users and the sites that users access. On our end all the server sees is a dummy IP address that is associated to the client server. Therefore, the students are already visiting our site in a confidential manner.

The Core Institute cannot link IP addresses back to the students. Your university maintains the internal IP accounts and the Core Institute does not have access to your University's IP accounts, nor would your school ever give them to us. Your university does know student's internal IP addresses but it has no access to the Core Institute's data files or servers. We do not provide them with this information, nor could we since the IPs are not logged.

If students use DSL or a cable modem they may be directly linked. This means that the IP address seen on the web is actually the IP address of his or her machine, instead of a range of IP addresses used by a public or client server. These individuals usually have greater security concerns than persons who use a client server. However, even these individuals are protected since our server does not log IP addresses.

Finally, all information transmitted to the server is encrypted using 2048-bit SSL encryption under license with InCommon.

While we feel comfortable that the data is collected and maintained in an anonymous manner the themes within the survey can make some respondents feel a need for extra caution. Respondents concerned about privacy can try to utilize a company that deletes their user logs rather than use an anonymous proxy. This way they will not be excluded from the site and their confidentiality will be maintained. An alternative option is to use a public access terminal (ex. computer lab) that cannot be linked to any one individual. These two options would render any attempts to link the individual to the data useless.

The following are common instructions that should be given to students taking the survey on the web.
- Go to the World Wide Web address: https://coresurvey.com.
- Follow the prompts to enter your school's 5-digit code which is the same for all students participating at your school or (9-digit code which is unique for you). Your password will be randomly assigned to you on your initial login. If you are unable to finish the survey you will need to remember your password so you may complete the survey at a later time.
- There is no connection between your name and the generated password, so do not lose or forget it. We cannot provide it to you again. The password is the only link to your data, not your name, nor your user ID.
- Once you complete your survey it is locked out. Access is denied even with the password.
- We recommend you complete the survey in a single session to ensure the greatest level of security.