Statement of Compliance with University Policy on Personal and Confidential Information

All users of the Demography Lab must be in compliance at all times with the campus policies regarding the storage of confidential personal information on computer systems.

Relevant policies cover two types of data: financial data, protected by California Senate Bill 1386 (SB 1386) and student data covered by the Federal Family Educational Rights and Privacy Act of 1974 (FERPA)

Campus policy relating to SB1386 is summarized at:
`http://cphs.berkeley.edu/policies_procedures/ga106.pdf` Campus policy relating to FERPA is summarized at:
`http://registrar.berkeley.edu/academic-policies-procedures/ferpa`

The Demography Lab requires that all users review these policies and agree in writing to comply with them by following two rules:

1. **Never store any data protected by SB1386** An examples of protected data is an individual's first and last name in combination with any of following:
   - social security number,
   - driver's license number,
   - financial account or credit card number in combination with any password that would permit access to the individual's financial account.
2. **Keep all student records confidential** An example of a violation of FERPA would be to post student grades with student id numbers. Student id numbers **are** considered personally identifying.

I assume full personal responsibility for all data that I store on the Demography Lab computers. I have read and understand the campus policies on personal financial and academic data. I agree to follow all campus policies relating to personal data. And I agree to abide by the two rules enumerated above.

I also understand that the Demography Lab routinely logs information necessary to comply with security alerts including logs generated by DNS,SMTP,IMAP,sshd, firewall, and maybe other things too. In some cases it might be possible to define these records as personally identifying. Such practices (and this announcement) are all in compliance with University policy set forth in

`http://policy.ucop.edu/doc/7000470/ElectronicCommunications`
`https://security.berkeley.edu/security-policy-nat-devices`
`https://ethics.berkeley.edu/privacy/regulations`

Name: _____ Date: _____

Current email address: _____
(all mail to you@demog will be forwarded to this address)

Preferred userid: _____ **TEMP** password (letters and numbers): _____

Phone number capable of receiving SMS text messages:_____
(If your temporary password is inadequately secure we will create one and text it to you)

Signature: _____

Please contact Carl Mason if you actually need to store protected data on the system.