**Use of UCL student and staff Personal Mobile Devices for Research Purposes**

1. The use of personal mobile devices presents risks, in particular:

* the device is lost or stolen with sensitive data on it;
* information not being adequately destroyed or being used for the wrong purposes;
* UCL having less ability to monitor or control the data, such as information is stored in personal cloud storage.

Accordingly, the presumption is that device or systems used by UCL should be owned and/or managed by UCL, with adequate security systems in place. In nearly all cases it is not necessary and not advisable for UCL staff and students to use personal mobile devices for research purposes.

1. If a staff member or student requires a mobile device, then they should undertake reasonable efforts to obtain one from their business unit, and the business units should undertake reasonable efforts to obtain a mobile device if it is necessary. If sensitive data is to be collected on a mobile device, it must be used in accordance with UCL’s [privacy policies](https://www.ucl.ac.uk/legal-services/privacy).
2. Alternative methods other than using personal mobile devices should be considered, and ISG should be consulted if staff and students have concerns about collecting and storing personal data. For example, MS Teams should be considered, as that can be accessed on staff devices and can call external parties.
3. Special category information must not be stored on personal mobile devices, and should not be stored on UCL portable devices in general.

**If personal mobile devices must be used**

1. There may be possible rare scenarios where the use of personal mobile devices may be necessary. This should only be in rare one-off scenarios and not involve sensitive or large amounts of personal data (Possible example could be where staff members are travelling to meet participants and may need to update participants about travel delays in transit). Staff must ensure personal data is used in line with UCL’s [privacy policies](https://www.ucl.ac.uk/legal-services/privacy/ucl-staff-privacy-notice).
2. Adequate and updated security safeguards/systems should be in place on the mobile device, for example PIN/password protection, encryption, and antivirus. Any data breaches must be promptly reported (Please see how to [Report a Breach of Personal Data](https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/report-breach#reporting)).
3. In these cases, care should be taken to ensure personal data is kept safe, and is not stored permanently on personal devices or in personal cloud storage (personal data should stored and backed up in UCL systems). Any Information such as contact details and messages should be deleted promptly when no longer needed and/or transferred as soon as possible to a UCL device.
4. Where possible, anonymising or pseudonymising the data should considered to reduce risk.
5. As with any personal data obtained in the course of their duties, staff members must not use the personal data for personal or unconnected purposes.
6. Please note, for research there may be additional requirements beyond data protection imposed by ethics, such as providing personal contact information to participants, or the research funders.