UCL students processing personal data overseas – guidance

Introduction

Following the impact of the global Coronavirus pandemic, many of UCL's students will at least start their teaching in Academic Year 2020/21 from outside the UK – and many of those from outside the EU.

As part of their course, many students need to process personal data – eg by research methods involving surveys or manipulating data which is already held by UCL.

Therefore, questions have been raised as to whether students are allowed to undertake research activities using personal data when based outside the UK and, if so, what protections should be put in place.

Issues

UCL has responsibility for all personal data processed under its control – including by students. Therefore it must ensure that any processing of personal data is completed in accordance with relevant data protection legislation. In the context of UCL students accessing personal data overseas, there are two main questions which need to be addressed: Can UCL students access personal data overseas in accordance with the law and, if so, how should they.

Question 1: Can UCL students access personal data overseas in accordance with the law?

The ICO guidance on international transfers (which require additional legal protections) sets out specific criteria for determining whether a restricted transfer is occurring. These are as follows:

- The GDPR applies to your processing of the personal data you are transferring;
- You are sending personal data, or making it accessible, to a receiver to which the GDPR does not apply. Usually because they are located in a country outside the EEA; and
- The receiver is a separate organisation or individual. This includes transfers to another company within the same corporate group. However, if you are sending personal data to someone employed by you or your company, this is not a restricted transfer. The transfer restrictions only apply if you are sending personal data outside your organisation.

In the case of restricted transfers, students can be treated on the same basis as employees. This is because UCL are the data controller for the data processed by students (ie, we take eventual responsibility for the data) and the student remains part of UCL when processing the personal data. Therefore, the personal data is not being transferred to a separate individual or organisation.

Therefore the answer to question 1 is yes. UCL students can access UCL personal data overseas in accordance with the law.

Question 2: If UCL students can access UCL personal data overseas, how should they do so?

UCL still has a legal obligation to protect personal data in accordance with data protection law when students are processing personal data outside the EEA. There are particular data security risks when personal data is processed overseas and a UCL system is not used. For example, if data is stored elsewhere than on a UCL system, UCL cannot guarantee that personal data won't be accessed, altered, disclosed or deleted only by those it has authorised to do so; that the data is accurate and complete in relation to why it is being processed; and that the data remains accessible and usable.

For these reasons, we recommend that as far as possible when data is accessed by students overseas then such access is via the VPN or Desktop@UCL. The main advantage of both of these systems is that any data processing can take place on UCL systems and is covered by UCL's data security.

However, there may be situations in which personal data needs to be accessed by other means. An example of this is if students simply do not have access to the VPN due to load issues, or the nature of their internet connection means that it is too unstable to complete the work online and data must be downloaded locally to enable the student to carry out their research. Such access should only be on an exceptional basis, and should be approved by the student's supervisor. Supervisors can approve access outside the VPN when:

- It is impossible/highly impractical for students to access the VPN/Desktop@UCL;
- The personal data has been pseudonymised as far as possible (ie, all personal identifiers have been removed) before the data is sent to the student; and
- The supervisor has explored with the student whether data analysis can be conducted within a UCL system, such as Opinio or Redcap and concluded it would not be possible to do so.

If students are processing personal data outside of the VPN/Desktop@UCL, they must comply with UCL's Bring Your Own Device (BYOD) Policy. In particular, students must make sure they follow the guidance in the data protection training regarding handling, storage and retention of data. Personal data should only be sent to their UCL email account or shared using the N drive or UCL file share systems and should not be forwarded onto non-UCL systems. Students should ensure that any systems they use have up to date virus protection, are encrypted where possible and are never left unlocked. To the extent possible, students should ensure they only process personal data on a machine only they have access to – not, for example a shared computer. If a shared computer is used then students should ensure they set up a separate account on the computer, to which only they have the password for access. In addition, once the student has finished using the data, it must be deleted.

Conclusion

Students are permitted to access personal data outside the EEA. Such access should be via a VPN where possible (including Desktop@UCL). If such access cannot take place via a VPN, then supervisor's approval is required and appropriate security measures should be taken.