Data protection guidance for UCAS Progress

When using the UCAS Progress system, you are responsible for handling the personal data of your students in compliance with data protection legislation. We have provided guidance on how you can do this below.

Looking after your login details

- Once you have received your login details, please change them to something unique to you. You should use a strong password containing at least eight characters, including upper and lower case letters, a number, and special characters.
- Check the strength of your password on The Open University's website at www2.open.ac.uk/openlearn/password_check.
- Please do not share your login details with other people. If another member of staff requires access to the system, please direct them to your user manager so they can be set up as a user in their own right.
- Be careful to keep your password secure:
    - If you use the system in a classroom environment, be careful when inputting your password to ensure it is not seen by others.
    - Do not write down your password or keep it where it can easily be found, such as under keyboards, stuck to screens, etc.
    - Do not leave yourself signed in if you have finished using the system – you must sign out.
    - Do not leave your computer unattended when using the system.
- Change your password regularly, and **if you have any suspicion your login details have been compromised, please notify the UCAS Progress Support Team**.

Role-based access

- Users should be given access to the appropriate level of data they need in order to conduct the duties of their role. Setting up the appropriate role for the staff member will assist with this, making sure staff can only access the data for the students they are supporting.
- Limit the amount of user management roles so you have sufficient resilience, but higher access is only granted to employees who need it.

Information sharing

The personal data is gathered for the application process, and should only be shared with authorised third parties.

Hard copies

- If you need to print any personal data from the system, please ensure the handling of this data is secure.
    - **Do not** leave data in any open areas where it may be seen by third parties.
    - **Do not** take data out of your school, if possible. This will reduce the risk of confidential data being lost in transit.
    - **Do not** leave hard copy data in vehicles, or have it visible on public transport. If you do have to take it off-site, please use a secure method of transportation, such as a locked briefcase.
    - **Do** store hard copy data securely. We would advise a 'double lock' approach, keeping it in a locked draw in a locked room.

- Do not keep hard copy data for longer than needed. Please refer to your centre's retention policy and ensure this is enforced.
- Do ensure data is confidentially destroyed when you have finished using it.
- Do not allow others to see this data if they would not be able to access it via the system.

Inappropriate use of the system

- Accessing personal data where you do not have a legitimate reason to do so is a breach of the Data Protection Act.
- Please only access details of the students you are supporting in a professional capacity.

Subject access requests

- If a student requests access to any of their personal data, please action this in line with your own data protection policy and processes.