

# STUDENT GROUPS DATA PROTECTION

## SECTION 1

This section of the self assessment is to help you understand if your student group is compliant with data protection and with Durham SU's data protection and information security policy and privacy notices.

If you ticked any of these boxes, then your group's activities are probably not compliant with Data Protection law and Durham SU's data protection policy. Don't panic! This doesn't mean you can't do your activities, most of the time it just means making some easy changes. We're gathering this information so we know the common problems and can consider solutions that can be used across multiple groups. But if there was something here you can easily change, please do. We have resources, including template privacy notice text, presentations on data protection for student groups and a template sign-up sheet that you can use.

Over the student group reregistration period we are planning to ask groups reregistering to submit some information to us about their data practices so that we can identify shared problems and help groups find solutions. By completing the self-assessment now, we hope that your group will be in a better position to answer these questions during reregistration.

**Please tick if any of the below apply to your student group**



### **1. Collect personal data other than -**

- Students names
- Students email addresses

**NOTE:** PERSONAL DATA IS DATA THAT RELATES TO AN IDENTIFIED OR IDENTIFIABLE INDIVIDUAL. YOU CAN FIND OUT MORE ABOUT THIS DEFINITION ON THE ICOS WEBSITE [HERE](#).

### **2. Store students personal data anywhere other than -**

- Online storage e.g. google drive, which you could demonstrate was GDPR compliant if required (i.e. it is clearly stated in the T&Cs and your exec are aware and have copies)
- Durham SU website
- A locked spreadsheet on a secure device

**NOTE:** NOT SURE IF A PLATFORM YOU'RE USING IS GDPR COMPLIANT? IT SHOULD BE IN THE T&CS OR CONTRACT AND SHOULD INCLUDE PARTICULAR INFORMATION, WHICH YOU CAN FIND OUTLINED ON THE ICO'S WEBSITE [HERE](#)

### **3. You have no record of who in the group has access to personal data, and your exec could not quickly provide this information along with any student data you hold if required to**

### **4. Your group does not provide privacy notices, explaining how you will use the personal data you are collecting EVERY TIME you collect data, including taking photos or videos.**

**NOTE:** DURHAM SU HAS TEMPLATE SIGN UP SHEETS AND PHOTO/VIDEO PRIVACY NOTICES ON AVAILABLE FOR YOUR GROUP TO USE [HERE](#)

**5. Your privacy notice does not include a link to Durham SU's privacy pages ([www.durhamsu.com/privacy-policy](http://www.durhamsu.com/privacy-policy)) so that students can find out how to request deletion, change, copies of or object to the processing of their data.**

**6. Nobody on your group's exec has completed DUOs online data protection training**

**7. Nobody on your group's exec feels confident in taking the lead on your group's data protection as the main point of contact should a data protection query arise**

**NOTE:** YOU CAN IMPROVE YOUR KNOWLEDGE OF DATA PROTECTION BY UNDERTAKING THE UNIVERSITY'S DATA PROTECTION TRAINING ON DUO, READING THROUGH OUR TRAINING RESOURCES [HERE](#), OR VISITING THE ICO'S COMPREHENSIVE INFORMATION PAGES.

## SECTION 2

This section is to help groups recognise if they are at high risk of a breach of their members data protection rights, so that we can work with them as a priority to reduce this risk.

If you do any of the below, then your groups are probably not protecting your members data and you are at high risk of a data protection breach. This doesn't mean that you have necessarily done anything wrong as individuals - the law has changed recently so old practices may no longer be legal. Please get in touch with us immediately if you think your group is high risk, so we can meet with you and address how to make your students safer when they engage with your groups activities.

**Please tick if any of the below apply to your student group** 

**1. Your group believes that you may have a personal data breach in the past 12 months but has not reported it to Durham SU**

**2. Your group shares personal data with anyone outside Durham Students' Union (this includes Durham University staff or other students, as we are a different organisation)**

**3. Your group collects special categories of data (this include race, religion, age, sexuality, gender, disability, marital status, biometric data, criminal convictions)**

**NOTE:** ANY STUDENT CAN BE A MEMBER OF ANY STUDENT GROUP. THIS MEANS THAT MEMBERSHIP OF A STUDENT GROUP IS NOT CONSIDERED A SPECIAL CATEGORY OF DATA. FOR EXAMPLE, BECAUSE YOU DON'T HAVE TO BE DAOIST TO BE A MEMBER OF THE DAOIST SOCIETY, MEMBERSHIP FOR THAT GROUP IS NOT CONSIDERED A SPECIAL CATEGORY OF DATA.

**4. Your group transfers personal data outside of the EU**