How to... 
...comply with GDPR

What is GDPR?
GDPR is the General Data Protection Regulation implemented in May 2018.

Why is GDPR important for volunteers?
During your time volunteering with the Students Association, you may be given and then hold personal information that can identify another living person. It is the Students Association’s responsibility to control the way this personal data is stored and used. As a volunteer, you have a responsibility to follow the GDPR guidelines for your role. This How To... will be appropriate for most of our volunteering roles but for Student Leadership roles and for Trustees, the full OU online training on GDPR compliance will be required.

What is personal information?
All recorded personal data whether kept in electronic or paper form, including names, emails, phone numbers, photographs labelled with names, information gathered in application forms, are covered by this regulation.

Sensitive personal information includes data that reveals a person’s racial or ethnic origin, political opinions, religious belief, health, and concerning a person’s sex life or sexual orientation.

Why collect, maintain and protect data?
The Students Association maintains data on students in order to deliver the organisation’s aims. We ensure before collecting this data that the reason for the collection of the data is made clear to students. For example, there is a link to our Privacy Policy on our website (oustudents.com) when each student registers for an account.

We collect the minimum amount of information relevant to the purpose for which it will be used. The rule is that data must be adequate, relevant and necessary, and if personal data is to be stored, there should be a mechanism for making sure this data is secure, accurate and up-to-date.

GDPR is in place to protect living individuals from damage or distress caused by their data falling into the hands of someone who shouldn’t have access to it. Loss of data (it could be accidental or unlawful destruction, loss, alteration, unauthorised
disclosure of or access to personal data) could cause distress and extra work for the person affected. We require **explicit consent** to use sensitive personal data.

If the Students Association fails to comply with the data protection regulation or has a breach of security leading to personal data falling into the hands of someone who shouldn’t see it, then we can be fined up to the sterling equivalent of 20 million euros. All breaches **must** be reported to Alison Lunn and Rob Avann (The Association’s Deputy and Chief Executive) as soon as you become aware.

Alison and Rob need to assess the scale of the breach and determine whether or not it is reportable to the Information Commissioner’s Office (ICO) within 72 hours of the breach occurring. It is also important that we act quickly in order to minimise the effect on the persons concerned. It is a requirement that we log all breaches and actions taken to reduce the risk of harm to individuals, irrespective of whether the breach meets the threshold for reporting to the ICO.

**Minimising chances of any data breaches:**

**Do:**

- Ensure that you ask permission of any student in a photo if you intend to name them.
- Be mindful of only asking for data you will really need - use of personal data should be **specific, explicit and legitimate** (e.g. if your volunteer application will be seen by students on an appointment panel then you will be asked to provide approval for it to be used in this way).
- **Report immediately** to Alison Lunn (alison.lunn@open.ac.uk) and Rob Avann (rob.avann@open.ac.uk) if a breach has taken place and student data has been compromised.
- Know that individuals have a right to any corrections and complete erasure of all data held on them So only store data on OneDrive within your Office 365 account, and be prepared to provide access to this to the Association if requested.
- Use OneDrive within your Office 365 account to store and share data where appropriate.
- Follow and conform to the OU’s Student Computing Policy to ensure **personal data is securely kept** – including keeping your devices physically safe and malware protected.
- Delete, dispose of securely or anonymise personal data as soon as it is no longer required for the purpose for which it was collected.
- Adhere to the Volunteer Agreement.

**Don’t:**

- Email a group of students without using ‘Bcc’ – the blind carbon copy line - otherwise, other students will see everyone’s personal email address.
- Write down on a piece of paper all names and phone numbers of students attending an event as the paper may be read by others and could be lost.
• Store student personal details on your personal devices. Personal data may only be stored in places accessible to the Association. Therefore if you need to store personal data, it must be within your OneDrive account.
• Ask students for personal information that you don’t need for a particular role (e.g. asking a student for their political views on an application form for a Graduation Volunteer is not considered as **lawful, fair and transparent** processing of data).

**And remember**, don’t keep data for longer than is necessary and dispose of that data as appropriate and as directed.

**Queries**

If you suspect a breach, don’t delay and contact Alison Lunn and Rob Avann immediately at (alison.lunn@open.ac.uk and rob.avann@open.ac.uk)

For general queries on GDPR, please contact the Volunteering team at oustudents-volunteer@open.ac.uk