

**DUVO Data Protection Policy**

**Introduction**Any Durham University Volunteering and Outreach Staff, or Staff and student volunteers who handle the personal data of others must complete the University’s information Security and Data Protection Training before being allowed to handle personal data.
The link to the training can be found here:
[**Learning Catalog - Learning - Oracle Fusion Cloud Applications (oraclecloud.com)**](https://ehjb.fa.em2.oraclecloud.com/hcmUI/faces/FuseWelcome?_adf.ctrl-state=26ty1ypbw_1&_adf.no-new-window-redirect=true&_afrLoop=54129519617171226&_afrWindowMode=2&_afrWindowId=null&_afrFS=16&_afrMT=screen&_afrMFW=1233&_afrMFH=609&_afrMFDW=1280&_afrMFDH=720&_afrMFC=8&_afrMFCI=0&_afrMFM=0&_afrMFR=144&_afrMFG=0&_afrMFS=0&_afrMFO=0)

This includes but is not limited to Project Leaders, College Volunteering Coordinators and DUVO Staff.

The fact this training need to be completed should be conveyed to Project leaders as part of their training for the post.

The Below Information details some essentials every individual should follow to supplement the university’s training.

**Principles of data protection**

The essence of the Data Protection Act is its eight data protection principles. Each of these principles puts obligations on the data controller to make conscious decisions on how it collects, holds and uses personal information.

The eight principles make clear that personal data shall be:

* **Processed fairly and lawfully**. The data controller must seek to receive consent from data subjects for processing and demonstrate that the processing is necessary. In the case of sensitive personal data consent should be explicitly recorded.
* **Processed for limited defined purposes**. Before seeking consent for processing, the data controller must know why personal information is needed and for what it will be used. Otherwise you are not receiving consent. When new processing is considered you must make sure that the processing is consistent with what you previously received consent for or seek it anew.
* **Adequate, relevant and not excessive**. Collecting personal data just because you might need it is not justifiable. Make sure you have a legitimate use before collecting that is consistent with the first two principles.
* **Accurate and, where necessary, kept up to date**. The best source of information will be from the individual. If this is not possible the data controller should take reasonable steps to verify. Correcting inaccurate information is a fundamental right for individuals. Make sure that a process is in place to promptly correct information.
* **Not be kept for longer than is necessary**. Personal data that is no longer needed becomes a risk to any organisation that holds it. How do you know when personal data is no longer needed? The answer is based on the reason for which it was collected in the first place. When personal data is no longer needed for that purpose make sure it is securely destroyed.
* **Processed in accordance with individual’s rights**. Individuals have many rights under the Act. The most critical is the right to know what information is held about them and, as mentioned above, to correct inaccurate information. Individuals also have some rights to stop the data controller from processing information about them.
* **Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data**. The data controller must make sure that any data held is secure and only accessible to those whose job it is to use it. If personal data is lost or stolen or security breached you must report it immediately to the appropriate people.
* **Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data**. Contracting third parties to operate certain organisation functions is a very common practice for financial and logistical reasons. It is very important however to ensure that the country or territory where the third party is based has the same respect for personal data privacy before any personal data is transferred.

**Rights of The Individual under the Data Protection Act**

* **Express direct marketing preferences.**
Individuals can dictate whether and in what form the data controller can communicate with them especially in regards to marketing activities. In particular, in order to use electronic means of marketing (phone, fax, and email) the data controller must receive consent and always provide individuals with an easy way to stop receiving further communications. Although more expensive, postal communications do not require the same prior consent. As part of maintaining good relations with the public, the data controller should always try to contact individuals in the manner they prefer.

**Record Management**

The timeline of Record Management of personal data is as follows:

**Electronic records**

The main place we store electronic records is the SDrive, however emails are also electronic records so organisation of email accounts is also important.

When saving any document to the SDrive you should label it following these guidlelines:

1. Start with the date the record was created e.g. 010412 (1st April 2012)
2. Status (final, draft, version) indicated by F for final, D for draft and V for version followed by a number indicating whether it is the first, second etc. For example D1 would indicate it is the first draft of a document. Unless there is a good reason to it is better not to keep multiple version/drafts of a document.
3. Meaningful title e.g. AGM Minutes
4. If relevant, the date of the event which the document relates to e.g. AGM Minutes 120312 (minutes of the AGM held on 12th of March 2012.)
5. If relevant, the name of the author of the document e.g. MHolmes to indicate Melanie Holmes as the author.
6. If the document, such as a letter, is meant for a certain recipient you should include their name as well, either in the title or after the name of the author.

Once named the document should be filed appropriately.

When creating a new folder this should be named clearly and accurately with a title which makes sense to other people. The year should always be used where relevant e.g. for an annual event, so that it is clear what year the documents in the file refer to. The ideal is to have consistency across different folders concerning the same topic. For example if the folder for oSCArs 2011 contains folders on Invitations, Publicity and Nominations, the oSCArs 2012 folder should follow the same pattern (as long as the categories are still relevant).

**Questions to Ask when collecting personal data**

* Do I really need this information about an individual? Do I know what I'm going to use it for?
* Do the people whose information I hold know that I've got it, and are they likely to understand what it will be used for?
* If I'm asked to pass on personal information, would the people about whom I hold information expect me to do this?
* Am I satisfied the information is being held securely, whether it's on paper or on computer? And what about my website? Is it secure?
* Is access to personal information limited to those with a strict need to know?
* Am I sure the personal information is accurate and up to date?
* Do I delete or destroy personal information as soon as I have no more need for it?
* Have I trained my staff in their duties and responsibilities under the Data Protection Act, and are they putting them into practice?
* Do I need to notify the Information Commissioner and if so is my notification up to date?