

Data Sharing Agreement Between University of Chichester and University of Chichester Students' Union

1. Overview

- 1.1 The following agreement governs the provision of registered students' personal data by University of Chichester ("UC") to University of Chichester Students' Union ("UCSU") and identifies the purposes for which that data may be used.
- 1.2 In this agreement "data controller", "data processor", "personal data" and "sensitive personal data" shall have meanings as defined by the Data Protection act 1998 (DPA).
- 1.3 Both UC and UCSU are, individually, registered as data controllers with the Information Commissioner's Office (ICO). Both organisations shall be data controllers in common of any student personal data shared. This means that each will be separately responsible for its own processing and for ensuring that students' personal data is processed only for the purposes described in this document, the Student Data Protection Statement, or by subsequent agreement directly with the student.

Responsibilities for compliance with this agreement are as follows:-

UC: Chief Executive's Team

UCSU: Students' Union Trustee Board

2. How students' personal data will be used by UCSU

- 2.1 General membership administration including website single sign-on
- 2.2 Administration of elections
- 2.3 Administration of UCSU clubs and societies
- 2.4 Administration of student representation on UC committees, panels, boards and other representative bodies
- 2.5 Generation of demographic reports
- 2.6 Verification of students' identity
- 2.7 To allow email communications between UCSU and its members
- 2.8 To allow email communication between its clubs and societies members
- 2.9 To ensure the health, safety and wellbeing of students including issues pertaining to Safeguarding.

3. Information to be shared

- 3.1 UC will provide UCSU with the following registered student data, or subset of this data, from its student information database:

- Student ID numbers
- First names
- Last name
- Date of birth
- Gender
- UC email address
- Network account (facilitates access to UCSU Website)

- Nationality
- Programme of study
- Mode of study
- Location of study
- Year of study
- Fee status
- Photo images

3.2 UC will provide UCSU with the following information for undergraduate applicants who are “Unconditional Firm” (UF):

- First names
- Last name
- Personal email address
- Home address
- Date of Birth

3.3 Other personal data will be shared as follows:

- CCTV footage or bodycam images but only where this relates to safety, security or detection and prevention of crime.
- Student Support Care Plans may be shared but only where the explicit consent of student has been obtained.
- Incident logs maintained by UC and UCSU contracted Security staff.
- Between Student Support and Wellbeing, Conference & Accommodation, Support and Information Zone and UCSU in connection with 2.9 above.

3.4 Sensitive personal data may be transferred between UCSU and UC but only as specifically referenced in 2.9 and 3.3 above.

3.5 UC will provide data and will exclude the following students:

- Partnership students studying wholly or mainly (that is for more than half their time) at a partner institution where they are not our contracted student numbers.
- Research students at the writing up stage.
- Students studying outside the UK.
- Non-UK based distance learning students.
- “opt-outs” (see section 7 below)

4. Information Provision

4.1 Student information from the Student Information Database (SITS) as set out in paras 3.1 will be provided to UCSU or their contractually appointed agents (e.g. Data Processors – currently Membership Solutions Limited (MSL) provide the UCSU website) securely by Corporate & eLearning Systems via an automated feed every night that ensures that mailing lists remain up-to-date. UC will transfer up-to-date information and the details of any student who has opted out of membership of UCSU will not be included.

- 4.2 Student information from the Student Information Database (SITS) as set out in paras 3.2 will be provided to UCSU or their contractually appointed agents (e.g. Data Processors) securely by Admissions.
- 4.3 Where data has been entered directly to the UCSU website there will be an end-of-year review of data to ensure that it is accurate. This applies to such data as e.g. Student Academic Representatives, membership of a given Club or Society etc. All memberships are deleted via an annual automated process within the MSL website.
- 4.4 UC Admissions & Academic Registry and Planning will provide additional, ad hoc student information on request and by agreement with UCSU, taking into account the operational requirements of UCSU and UC.
- 4.5 Where a student informs UCSU of a change to any of their personal data held on SITS, UCSU shall inform the student of how to update this change within UC procedures.
- 4.6 An agreed list of UCSU staff will be given up to Level 2 (applies to roles with a remit which includes making contact with students) access to the student portal (SONAR). This list will be reviewed annually to ensure it remains current, by UCSU and any changes notified to UC.

5. Data Transfer and Security

- 5.1 Both UC and UCSU will ensure that all personal data shared under this agreement will be kept secure and protected against unauthorised access, use or disclosure. In particular, information about identifiable students will only be made accessible to Data Protection trained UCSU staff members who necessarily need access to that information for the purposes specified in this agreement. If UCSU becomes aware of any potential data breach of security which involves data supplied by UC, it must be raised with UC immediately.

6. Conditions for processing student personal information

- 6.1 With regard to the use of students' personal information, UCSU is to ensure:
 - 6.1.1 Compliance with UC's Data Protection Policy and guidelines where appropriate.
 - 6.1.2 Compliance with the eight data protection principles in the Data Protection Act 1998 generally.
 - 6.1.3 Only UCSU trained staff will have direct access to personal information and UCSU approved and trained third party contractors such as security staff may be provided with personal information as required in connection with paras 2.6, 2.9 and 3.3.
 - 6.1.4 Members of UCSU staff handling student personal information have undertaken UC's on-line Data Protection course as part of UC's staff development programme. Any data processor UCSU uses has security policies and procedures that ensure compliance with Principle 7 of the Data Protection Act 1998.

7. Restriction on the use of information

- 7.1 The information provided by UC to UCSU shall not be passed to any third party (data processors excluded) without the express consent of the individual(s) concerned, except where UCSU has obtained the written permission from the Data Protection Officer or Deputy Vice-Chancellor.
- 7.2 Should student personal data be released to a data processor to host UCSU's website, UCSU shall ensure that the data processor is contractually:
- 7.2.1 Restricted from using the data for any other purposes other than those UCSU purposes set out in para 2 above.
 - 7.2.2 Obligated to comply with conditions in para 6 above.
- 7.3 The information provided by UC to UCSU shall not, without the express consent of the individual concerned, be used for the purpose of marketing products or services of external organisations or individuals other than UCSU.
- 7.4 Students are given the option by UCSU in each direct mailing from the UCSU systems to opt out of receiving future mailings and may do so at any future point by contacting UCSU and requesting to be removed from the electronic marketing system.
- 7.5 Information sent to students relates directly to the operational activities of UCSU or to products and services provided by UCSU which are of genuine benefit to students.

8. Student opt out rights

- 8.1 The following opt out procedures shall be in place:

In relation to para 4.1:

- 8.1.1 If a student notifies via the registration or re-registration processes that they do not wish to be a member of UCSU then their personal information will not be included in the overnight transfer of information process.

In relation to para 7.4:

- 8.1.2 Where a student has opted out of data sharing, UCSU (or any data processors working on behalf of UCSU) shall ensure that their personal information is destroyed and no longer processed immediately on being informed by the student.
- 8.1.3 UCSU shall maintain a mechanism for students to opt out of receiving marketing information but remain on the Membership database for purposes connected with paras 2.2 and 2.9 above.

9. Retention of information

- 9.1 Personal data must only be kept for the length of time necessary to perform the processing for which it was collected. This applies to both electronic and non-electronic personal data. UCSU will ensure that retention policies are adopted to ensure that the student personal data specified in this agreement is destroyed once no longer needed. In most circumstances personal data will only be retained for the duration of membership of UCSU, i.e. once a student is de-registered, completes a course of study or after graduation as appropriate UCSU will destroy all data held.

9.2 Non-current system student data will be deleted on an annual house-keeping basis with the exception of University student ID number and transactional data, which will be retained in accordance with Financial Regulations, however,

9.3 Exceptions to this are:

9.3.1 Where during their membership students have participated in extra-curricula activities administered and verified by UCSU which may be included in schemes such as the Higher Education Achievement Report.

10. Review and publication

10.1 The operation of this agreement will be reviewed annually by the UC Data Protection Officer and the UCSU General Manager in June/July of each year. If no changes are required, re-confirmation may be by email from the UCSU General Manager and the UC Data Protection Officer to the Chief Executive's team (ChET) and the UCSU Trustee Board. It may also be reviewed at other times if it is necessary to add a new type of data processing to the agreement or to make other urgent changes and on these occasions approval by ChET and the UCSU Trustee Board will be required.

10.2 This agreement will be published on the UC and UCSU websites and a link will be included in the University's Student Data Protection Statement.

11. Indemnity

11.1 Each party shall indemnify the other against all liabilities, costs, expenses, damages and losses (including but not limited to any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs and all other reasonable professional costs and expenses) suffered or incurred by the indemnified party arising out of or in connection with the indemnifying party's breach of any of clauses 2, 3.3, 3.4, 5, 6, 7.1, 7.2, 7.3, or 9 of this agreement.

11.2 This indemnity shall not cover the indemnified party to the extent that a claim under it results from that party's negligence or wilful misconduct.

11.3 Nothing in this clause 11 shall restrict or limit either party's general obligation at law to mitigate a loss it may suffer or incur as a result of an event that may give rise to a claim under this indemnity.

Other useful links:

Data Protection:

<http://www.chi.ac.uk/about-us/how-we-work/policies/data-protection>

Electronic Information Security Policy:

<http://www.chi.ac.uk/about-us/how-we-work/policies/it-and-information-policies>

Under-18 Policy:

<http://www.chi.ac.uk/about-us/how-we-work/policies/academic-policies>

Safeguarding:

<http://www.chi.ac.uk/study-us/student-services/policies-and-guidelines>