UNIVERSITY OF KENT'S OUTREACH INFORMATION SHARING AND DATA PROTECTION POLICY

This policy has been constructed to ensure that the data collected as part of the University of Kent's outreach provision, led by the Partnership Development Office (PDO), complies with the requirements of the Data Protection Act 2018 ('the Act') and the General Data Protection Regulation (GDPR).

1. Introduction

1.1 The University of Kent ('the University') collects, processes and stores information about the outreach participants, Schools and FE Colleges with whom we work in order to administer and evaluate activities and track educational progression of participants. The University also processes information relating to student ambassadors for the purposes of monitoring, evaluation and administration of the ambassador scheme.

1.2 When handling such information, all University staff or others who process or use any personal information on its behalf, must comply with the Data Protection Principles set out in the Data Protection Act 2018 ('the Act') and the General Data Protection Regulation (GDPR).

1.3 All University staff or others who process or use any personal information, must ensure that they follow these principles at all times. This policy sets out the ways in which we will ensure that these principles are put into practice.

2. Policy Scope

2.1 This policy applies to:
2.1.1 All PDO staff
2.1.2 All University Academic Schools and Centres who contribute to the delivery of the University's outreach activities
2.1.3 All University Partner and KMPF Schools and Colleges
2.1.4 All University Community Partners
2.1.5 All Schools, Academies and Colleges who participate in the University's outreach activities

2.2 The University collects information about the students participating in outreach activities in order to track the proportion who subsequently enter higher education, their degree qualification and employment prospects upon graduation. This enables us to evaluate and improve the programme of activities, as well as report to local funders and relevant national bodies.

2.3 The University takes photographs and videos at outreach events for use in marketing and promotional materials. Photographs and videos where individuals are clearly identifiable are covered under this policy.

2.4 Personal information will be collected through student baseline forms, post-activity questionnaires, activity attendance records or any other form associated with outreach provision. This information includes:

i) Full Name
ii) Date of Birth
iii) Gender
iv) School Name
v) Parental Educational background
vi) Postcode
vii) Qualitative baseline data regarding participants' attitudes and perceptions of education, particularly higher education.
viii) Photographs and videos at outreach events

The following data of sensitive nature will be collected and processed by PDO for the sole purpose of equality monitoring; with the aim to help eliminate disparities in access and progression to Higher Education:

ix) Ethnicity
x) Disability

3. Data Ownership and access control

3.1 All information hosted and processed by the University regarding students, and other data subjects for academic, administrative and commercial purposes must be in accordance with the University's Data Protection Policy, which in turn, needs to comply with the Act and GDPR.

3.2 The Act and GDPR applies to data held in manual paper files as well as on electronic systems. To comply with the Act and GDPR, information must be collected and used fairly, stored safely and only disclosed lawfully to a third party.

3.3 The University holds a data sharing agreement with all its outreach partners, namely the Kent and Medway Collaborative Outreach Programme (KaMCOP) and Kent and Medway Progression Federation (KMPF) partners regarding the sharing of data for the purpose of monitoring and evaluation. The signatories of the data sharing agreement will be **joint data controllers** of personal information they share with each other. This means that they will as far as practicable collaborate on the collection of personal data (to avoid the need for data subjects to provide data twice). This agreement is available on the University's website, or by emailing pdodataprotection@kent.ac.uk .

4. Data Processors

4.1 All data processors must comply with the Act and the GDPR.

4.2 If any processing of University's outreach data is required to be performed by any third parties, the University will ensure that this is consistent with the purposes for which the data was collected. The University will ensure that a data processor agreement, compliant with current and future data protection legislation, is in place before any processing takes place. The Data Processors should be named on any data privacy notices.

5. Policy Aims

5.1 This policy has been constructed to meet the commitment to Principle 7 in the DPA*, protected by appropriate security*, and Chapter 2 Article 5 (f) of the GDPR*,* listed above. It is concerned with the handling of information related to the University's outreach work (as outlined in section 1.1) and the processes outlined below:

a) The submission of information (including emails, forms, folders, invoices) to the University electronically, in person or through postal delivery;
b) The storage of information held in manual paper files as well as on electronic systems;
c) The distribution of this information to third parties either in person (e.g. through the distribution of reports at meetings), by post or electronically (e.g. by e-mail or through a designated website);
d) The disposal of information;
e) The University's policy towards employees with access to outreach information.
f) The retention of outreach participants' data

6. Data Retention

6.1 No data will be shared with other institutions or retained on the HEAT database once the related retention period has expired (see section 13).

6.2 The retention period is the intended amount of time data should be kept in order to be processed for any purpose or purposes and which shall be no longer than what is necessary for that purpose or those purposes. As per guidance from the Office for Students (OfS), the University will be required to retain personal data (excluding photographs and videos) for the following periods:

6.2.1 Young Students
Where a data subject is NOT deemed 'Mature' (aged 21 or over) when first entered on to the HEAT database their data is retained until they reach 30 years of age. If that individual enters HE during this period of retention then their data is then retained for a further 15 years from graduation. If a student does NOT enter HE by the time they reach 30 years of age or has been tracked for 15 years from graduation, an extract of their data is retained in a de-identified/anonymised dataset for secondary research purposes only.

6.2.2 Mature Participants
Where a data subject is aged 21 or over when first entered onto the HEAT database, their data will be retained for 10 years. If that individual enters HE during this period of retention then their data is then retained for a further 15 years from graduation. If a mature participant does NOT enter HE within 10 years of taking part in their first outreach activity

or has been tracked for 15 years from graduation, an extract of their data is retained in a de-identified/anonymised dataset for secondary research purposes only.

6.3 For students enrolled on programmes accredited by The Open College Network South East Region Ltd (trading as 'Laser Learning Awards') the University will retain documents and records for a period of six years. As a national awarding organisation regulated by QAA (for Access to Higher Education Diplomas) and Ofqual (for all other national qualifications), Laser are required to maintain student records for the 'lifetime of learners'.

6.4 Photographs and videos taken at outreach events (see section 2.3) will be stored electronically for a period of 6 years, during which they may be used for marketing and promotional materials. After 6 years, photographs and videos will be archived. Archived photographs and videos will only be used for historical and research purposes.

7. Legal Basis for Processing Data

7.1 All personal data will only be processed in accordance with Principle I of The Act on the basis of one or more lawful conditions for processing. The University recognises the high social value and public interest related to the Office for Students' objective that 'all students, from all backgrounds, with the ability and desire to undertaken higher education, are supported to access, success in, and progress from higher education. The University considers obtaining participant's information as integral to carrying out the necessary evaluation of the University's outreach programme through longitudinal tracking on the HEAT database. If personal data should be processed as a public task according to Article 6(1)(e) of the General Data Protection Regulation, the University will evaluate the compliance of this lawful condition for processing with the limitation stated by the same Recital on unbalance of powers.

7.2 Where University employees, schools or FE colleges collect data on the University's behalf, the University will ask employees / participating schools / academies / colleges to explain to pupils (and parents where needed):

- Why their data is being requested;
- How long their data will be stored for (as per section 6);
- The need for data sharing between KMPF and KaMCOP delivery partners (for example, to store student information on the database administered by the Higher Education Access Tracker service);
- The essential need for data sharing with official custodians of education data including the Higher Education Statistics Agency, UCAS, the Department for Education, OfS and other agencies (for research purposes only);
- The need for data to be transferred in both directions from the school / academy / college to the University, and in reverse (for example, to advise schools which of their students fall within targeting criteria);
- How to obtain access to their own personal data or raise queries about how it is held.

7.3 Where consent is the lawful condition for processing the data, it will remain the responsibility of participating schools / colleges / academies to gain appropriate consent from students and parents **before collecting or providing any student information to the University, or allowing students to participate in University outreach activities**. The nature of consent required (e.g. parental consent / student consent) may vary over time, and will be dependent on the age of the student; in all cases schools must comply with the most up-to-date guidance set out by the Information Commissioner's Office (www.ico.org.uk).

7.4 Where consent is the lawful condition for processing the data, Schools / academies / colleges will be asked to keep hard copies of consent forms (which the University may ask to see) and provide written confirmation to the University that they have the necessary consent to share personal information with PDO for any students whom they wish to participate in University activities. If consent is not given, then information must not be collected or passed to the University.

7.5 If a person, or someone who is responsible for a person, whose data is processed by participating in University outreach activities requests the withdrawal of their personal information, the University will evaluate the legitimacy of the request. Upon evaluation of the request, if the University feels that it should be approved, all relevant personal information related to that individual will be removed from the HEAT database apart from that information necessary to avoid any new data related to the person who made the request being processed again in the future. The organisation receiving the request shall also notify all KaMCOP and KMPF partners of such removal if necessary.

7.6 Where photographs or videos are taken at outreach events (see section 2.3) consent is the lawful condition for processing the data.

7.6.1 For individual under 18 years of age at the time the photograph was taken:

For anyone under the age of 18, the University will require both parental/legal guardian and individual consent. If either the parent/legal guardian or the individual does not agree to the use of photographs or videos by the University for marketing and publicity materials, no photographs will be taken of the aforementioned individual. An electronic copy of written consent forms will be kept by the University until the photos or videos are securely destroyed, in line with the University's retention period for photographs and videos (see section 6.4).

7.6.2 For individuals 18 or over at the time the photograph was taken:

For anyone 18 or over, the University will require written consent for photos to be used in marketing and publicity materials. An electronic copy of written consent forms will be kept by the University for 6 years, in line with the University's retention period for photographs and videos (see section 6.4).

8. Method for transfers of personal data between PDO partners, and data storage

8.1 Personal data collected for the University's outreach purposes as specified in sections 1 and 2, will be imported to the HEAT database, administered by the Higher Education Access Tracker Service. Data will not be transferred outside the European Economic Area.

8.2 Any hard or electronic copies will be stored securely on University of Kent servers, and access to this data will be restricted.

8.3 For all University outreach beneficiaries, namely schools/colleges/academies, or University employees that collect data on the University's behalf, data will be shared in the following manner:

a) Postal submission of outreach participants' information

i) Any party wishing to submit personal information (e.g. Student Name, Date of Birth, School, parental background in HE) by post will do so using a secure system that provides a written record of delivery (e.g. Royal Mail Special Delivery or Recorded Signed For).
ii) Under no circumstances should information be submitted by regular post.
iii) When submitting information by post, this will be clearly labelled to show which College, Academy, School or University of Kent employee has sent it and will include the name of the sender.

b) Submission in person of outreach participants' information

i) All University of Kent employees are expected to submit any personal information in person no later than 24 hours after the data has been collected, unless agreement is given by the University in writing before the event.
ii) However, the party submitting the data must be aware that the responsibility for this information will remain with the submitting institution up to the point that written acknowledgement of receipt (either in receipt or e-mail form) of the information submitted is issued by the University. This responsibility includes maintaining the secure storage of this information in compliance with the Act, and the GDPR at all times (including in transit).

c) Electronic submission of outreach participants' information

i) Information may only be submitted electronically through the use of an approved secure system, to be advised through the University of Kent's Monitoring and Evaluation Team. For further information please email pdodataprotection@kent.ac.uk .
ii) Information is also transferred from the University team back to schools / academies and colleges using the same approved secure system.

9. The receipt of information by the University and University outreach partners

The following steps outline the process to be applied when information is received and stored by the University.

a) As soon as information is received by the University offices, an electronic acknowledgement of receipt will be issued to the submitting University outreach partner or University employee.
b) Both the submitting and receiving party will keep a copy of this receipt for future reference.
c) The University outreach partner will be responsible for the secure storage of any information prior to its submission to the University.
d) Once received, it will be the responsibility of the University to ensure that information is logged by an appropriate member of staff to ensure that accurate records are maintained and available on request (e.g. audit purposes).
e) Similarly, once in receipt of information from a University outreach partner or University employee, it will be the responsibility of the University to ensure that any information that is either awaiting processing or has been processed is stored in a secure location.

10. Information Storage

10.1 Student data is stored on the electronic **Higher Education Access Tracker (HEAT) database**, in accordance with the Act, and GDPR, and will be used in accordance with the data protection notice administered upon the collection of the data.

10.2 The HEAT database is held on secure computer systems which are subject to stringent physical and electronic access control mechanisms. A copy of the HEAT Data Protection Policy and Technical Compendium is available upon request by emailing support@heat.ac.uk.

10.3 The HEAT database is password protected and different permission levels are set up to ensure only a small number of named database users have access to information at area administration level.

10.4 All new and existing University staff who have access to information will be made aware of the conditions of this policy and sign a confidentiality agreement with Partnership Development Office (PDO) as lead department, which will be kept on file.

11. Ensuring Data Quality

11.1 All University outreach partners and University employees collecting participants' information are responsible for the quality of the data they are adding to the HEAT database.

11.2 Before adding data to the HEAT database, University staff will check that the information is accurate to the best of their knowledge. If sensitive information is being shared which could harm the subject if it was inaccurate, then particular care must be taken.

12. The distribution of information to third parties

12.1 Students' personal information will not be disclosed unless absolutely necessary and only for the purposes of monitoring and evaluating the programme or where there is a clear legal requirement to provide information. Student information will not be shared with anyone who is unauthorised.

12.2 The University outreach participant details will be shared with the **HEAT service** (see Section 10), hosted by the University of Kent, for the purposes of **storage, data monitoring and evaluation**.

12.3 For **research and monitoring purposes only**, participant details may also be shared with colleagues and educational partners, including the **Office for Students (OfS), the Department for Education (DfE), the Higher Education Statistics Agency (HESA), the University and Colleges Admissions Service (UCAS**), our partners (including **colleges, HEAT subscribers, and the Education and Skills Funding Agency)** and other educational services organisations with whom we have an information sharing agreement. This will enable us to evaluate the effectiveness of this activity as part of the government policy to widen participation in higher education and to develop future policy.

12.4 We will ask school partners to obtain appropriate consent for collecting and sharing students' personal information (see Section 7). Parents and students can opt out of student data recording and data sharing at any time by contacting pdodataprotection@kent.ac.uk .

12.5 Data will not be shared outside of the European Economic Area (EEA).

13. The disposal of information

13.1 Information kept in paper form will be retained, until it is scanned and saved electronically on a secure protected folder on The University's server. The paperwork must either be shredded or arrangements made for a special collection by those responsible for the safe destruction of confidential waste.

13.2 Data stored on the HEAT database will be securely deleted once it is no longer required (see Section 6). The HEAT service will be responsible for all data transfers within the system. The system complies with all aspects of the Data Protection Act (2018), and the GDPR. The system has been checked by the ICO and meets their standards and those required by the Data Protection Act. All Cloud-based services and backups are within EU as per point 83 in the ICO's data protection guide lines. https://ico.org.uk/media/for-organisations/documents/1540/cloud_computing_guidance_for_organisations.pdf .

Penetration testing is carried out by Nettitude on an annual basis, to ensure that security and data standards are of the highest order.

13.3 The PDO and HEAT will retain a written summary of the data destroyed either physically or electronically. The summary will contain details of data type e.g. questionnaire, baseline student data, the data held within it e.g. date of birth, home address, the time period the data refers to and the quantity. The summary will be produced on request by appropriate bodies (e.g. funding councils).

14. Data requests

14.1 Under the Act and GDPR, participants have the right to a copy of the data held about them by the University. If an individual or a school has any concerns about the use of data for the purposes described in this policy, or would like a copy of the data that they have supplied directly to the University, these requests should be made by emailing pdodataprotection@kent.ac.uk .

15. Review

12.1 This policy will be reviewed annually in conjunction with PDO outreach partners and the Data Protection Officer for The University of Kent.