



Data Sharing – University of Sheffield and US in Schools Partner Schools

The purpose of this agreement is to outline the categories of Personal Data collected from schools/colleges, the purposes for which Personal Data is shared between the University and school/colleges, and to set out measures for compliance with the Data Protection Laws.

Personal Data Collected

We collect the following information from each school/college;

- Full Name
- Date of Birth
- Year group
- Address
- Postcode
- School/College name
- Unique Learner ID
- Gender
- Ethnicity
- Disability details
- Looked after child / Care leaver status
- Young Carer status
- Estranged status
- First generation in the family to enter Higher Education
- Pupil premium/free school meals
- Pupils Grade data
- Any relevant individual circumstances
- Other equal opportunity monitoring information where appropriate

Purposes of Data Sharing

The University and the School/College agree to share and process Personal Data for the following specified purposes only:

1. To identify potential participants for the University of Sheffield Widening Participation programmes.
2. To ensure pupils meet our targeting criteria.
3. To plan and administer activities.
4. To monitor participation in activities.
5. To evaluate and report both internally and externally on the effectiveness and impact of our outreach activities and other questions related to participation and progression which may be in the public interest.
6. To enable longitudinal analysis of changes in individual participants' attitudes, aspirations, knowledge about and intentions to apply for higher education.
7. To enable offers of additional support and other initiatives strictly to the benefit of the participant.
8. To understand the student journey through education and progression to Higher Education/future careers.



Obligations – Schools and University

1. In order to identify a potential cohort of pupils from our partner schools, school coordinators will complete an upload template with a potential cohort to provide full details of the young people they anticipate nominating for the programme. This list will include data relevant to our targeting criteria, such as home postcode, disability status and their current end of year levels, to allow us to ensure that each young person selected meets the targeting criteria for the programme. US in Schools Mentoring uses Outreach Online to identify a potential cohort and administer the application process as well as an individual Google Drive folder for each school participating in the programme. Access to Outreach Online and the Google Drive folder is limited to the Strategic Coordinators, Operational Coordinators, and Data Managers (or nominated staff member), staff at the University of Sheffield who work in UK Student Recruitment and Widening Participation as well as Epigenesys (developers of this system) to ensure the security of this data.
2. The school will provide individual pupil actual grades/levels (end of previous year), predicted levels/grades (for the end of the mentoring year) to the USiSM Team at the start of the programme, and actual levels/grades after the end of year exams to enable accurate monitoring of the programme's impact on participating pupils.
3. The University will upload elements of this data (*following pupils agreement to this during the application process and them accepting their place on the programme*) onto our HEAT database and then report the 'Shared Data' as aggregated data or, in the case of data collected through interviews and focus groups, anonymously and using pseudonyms. Exceptionally, the University can report the 'Shared Data' to the School/College in a non-anonymised way if this reporting is required for the performance of a particular public education task carried out in the public interest by the School/College. The University can provide the School/College with an annual report about the use of the supplied Personal Data to enable the School/College to account internally and externally on the use of the Personal Data in an aggregate manner.

The University and the School/College shall act as a Controller in respect of the processing of the personal data on its own behalf and in particular each shall be a Controller of the personal data acting individually and in common. Each party must:

- Ensure compliance with the Data Protection Laws at all times;
- Each manage its own costs in relation to compliance with the Data Protection Laws;
- Ensure that the shared Personal Data is: adequate, relevant and not excessive in relation to the processing purposes; accurate and maintained up to date; not kept for longer than necessary;
- Only share Personal Data of pupils who have been informed in advance of the Data Sharing (by way of an information sheet publicised by the school/college or the USiSM signed application form); the party conducting the primary data collection must communicate to the pupils the Privacy Notice;
- Not publish the Shared Data in identifiable form unless the concerned Data Subjects have given their consent and in conformity with other safeguards laid down by the Data Protection Laws and any other UK laws;
- Not copy, broadcast or disseminate the Shared Data to any third party unless provided in this agreement or if the disclosure is required by law;
- Employ appropriate technical and organisational measures, processes and procedures to ensure secure data transfer between them and keep the Shared Data safe from unauthorised use, access or disclosure, accidental or unlawful destruction, loss, alteration or theft;



- Not use the Shared Data in a way that would support decision making about the Data Subjects, with the exception of the application for the processing purpose enabling offers of additional support and other initiatives strictly to the benefit of the Data Subject;
- Restrict access to the Shared Data to those of its employees and volunteers who are directly involved in the Processing of the Shared Data or in providing technical support to those Processing the Shared Data;
- Ensure that all its employees and volunteers who Process the Shared Data have received appropriate training about their responsibilities under the Data Protection Laws and this agreement;
- Not engage a subcontractor to Process the Shared Data without the prior written consent of the other parties;
- Maintain complete and accurate records in relation to the Processing of the Shared Data and supply the other parties on demand and without undue delay with any reasonably requested evidence about its Processing of the Shared Data, including of any subcontracting, in order to demonstrate compliance with this agreement and the Data Protection Laws;
- Notify the other parties of a security breach, loss of Shared Data or a similar incident affecting data protection as soon as possible and, at the latest, within three Working Days from identifying the incident;
- Provide reasonable assistance to the other parties as necessary to enable them to comply with data subject access requests and to respond to complaints or communications related to the Processing of the Shared Data;
- Not transfer the Shared Data outside the European Economic Area;
- Retain the Shared Data securely for the duration of the Retention Period;
- This agreement shall be in force until 31 July 2021 and the University and the School/College shall review it every 12 (twelve) months and they may continue, vary or terminate it as a result of the review. Any variation to the agreement must be done in writing.

Glossary of Terms

"Data Controller"	a person or organisation who (either alone or together with other persons) determines the purposes for which and the manner in which any Personal Data is Processed.
"Data Protection Laws"	means: (i) the EU General Data Protection Regulation 2016/679 (GDPR) and any applicable national legislation that complements or supplements it, as amended from time to time; (ii) the Data Protection Act 2018 to the extent that it relates to Processing of personal data and privacy; and (iii) all applicable national legislation and authoritative guidance about the Processing of personal data and privacy.
"Data Sharing"	means the disclosure of Personal Data from one party to another or the others which results in the joint or separate Processing of Personal Data by the Universities and the School/College for any one purpose of a range of purposes expressly specified in this agreement.
"Data Subject"	a student at a school or a college in the Sheffield City Region, who is subject to the outreach activity of the Universities.
"Deletion"	erasing and destroying the Personal Data or putting the Personal Data beyond use.
"HEAT Database"	a secure online database and a specifically designed tool that enables standardised and bespoke data collection for subscribers.
"Personal Data"	information relating to a Data Subject who can be identified directly or indirectly from this information.
"Process" and "Processing"	any operation or set of operations which is performed on the Personal Data, such as collection, recording, organisation, structuring, storage, adaptation or



	alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction or deletion.
"Retention Period"	means the duration periods, subject to annual reviews as the project develops and in line with guidance from the Information Commissioner's Office and other best practice in the sector, as follows: a. if the Data Subject is below the age of 21 at the time of First Intervention, the retention period of that Data Subject's data is 15 (fifteen) years after the Data Subject's graduation or until the Data Subject reaches the age of 30, whichever is later; and b. if the Data Subject is aged 21 or over at the time of First Intervention, the retention period of that Data Subject's data is 10 (ten) years after First Intervention or 15 (fifteen) years after graduation, whichever is later. c. The length of the duration periods in (a) and (b) is required to enable the Universities and HEPPSY+ partnership to assess whether the outreach activities have been successful in widening participation in higher education.
"Shared Data"	the Personal Data Processed through the Data Sharing.
"Working Day"	Monday to Friday inclusive save for UK bank and statutory holidays and other days when the parties are not open for business, such days to be notified in advance by each party to the others.

Platform for Secure Data Sharing - Outreach Online and Google Drive

Why do we utilise online data collection via Outreach Online and an individual school Google Drive folder?

It will:

- Improve the accuracy and ease of collating pupil data, by keeping all records in one place that all relevant parties can view and update at the appropriate time;
- Improve impact evaluation and pupil destination tracking by collecting accurate participant data for the HEAT[1] database
- Ensure greater security of information by removing need for back and forth data submission via email and paper programme applications.

Strategic Coordinators, Operational Coordinators, and Data Managers for each school will be given an account with Outreach Online. Each school will also have its own Google Folder on the University of Sheffield's Google Drive. Strategic Coordinators, Operational Coordinators, and Data Managers (or nominated school staff) will be given editing rights to their school folder. Assigned Lead Mentors will be given editing rights to the 'Mentee Weekly Register' **only** within this folder, which they will complete following the weekly session for their corresponding school.

The USiSM Team will also have access to Outreach Online and all school folders. In order to access the google folder, each relevant member of school staff will need a Google Account. In order to access Outreach Online, each relevant member of school staff will need an account with a separate log in and password.



What will be stored in your school's Google folder?

The folder will be a hub for programme information and attendance data shared between the school and the University of Sheffield. This means that when the USiSM team/school coordinators send emails, they will not send attachments but instead refer coordinators/the USiSM team to the document title in their Google Drive folder or the relevant area of Outreach Online. This also means that any amendments that need to be made to data will also all be done online rather than via email.

General Data Protection Regulation (GDPR) guidelines/agreement from schools

- Ensure that it is only the Strategic Coordinator, Operational Coordinator, and Data Manager (or designated and approved school staff) who has editing rights and access to your school folder or Outreach Online; do not add any other additional members of staff.
- Do not share the link to the folder with anyone other than the above. Be mindful when sending emails that you do not accidentally share any link with contacts other than the above and the US in Schools Team.
- Keep us up to date if members of staff responsible for USiSM mentoring change throughout and at the end of the year, so we can update editing and access rights to your folder.
- Do not use your personal email account to sign into your school's google drive area; use your official school email address so that any data protection issues would be covered by the school GDPR Policy.
- Please read the University's policies below for more guidance on using a shared online drive.

The University of Sheffield Data Protection Information on Google Drive Use:

- IT Code of Practice: <http://www.sheffield.ac.uk/cics/codeofpractice>
- TUoS Data Protection Policies: <https://www.sheffield.ac.uk/govern/data-protection>
- Data Protection guidance when accessing Google Drive on remote devices: <https://ico.org.uk/your-data-matters/online/smartphone-security/>
- Advice on safe computing: <http://www.sheffield.ac.uk/cics/security>
- Data Protection Statement with Google Drive:
http://shf.ac.uk/polopoly_fs/1.254519!/file/FactSheet-DataSecurityandPrivacywithGoogle.pdf

Help when using Google Drive

- TUoS Guidance on How to Use Google Drive - <https://www.sheffield.ac.uk/it-services/google/drive>
- Google Drive introduction from Google - <https://support.google.com/drive/answer/2424384?hl=en>

[1] The Higher Education Access Tracker (HEAT) Service is a monitoring and evaluation service for member universities. The service encompasses a number of outputs including data management, analysis and reporting. Underpinning the service is a collaborative database to provide a web based data capture system that tracks student engagement in outreach activities delivered by each subscriber HEI and by partnership projects. (HEAT, 2015 available at: <http://heat.ac.uk/>)