



Privacy Notice

Though pertaining specifically to the collection and processing of data for the purpose of delivering the **HEAT Service** to subscribing members, the **HEAT Service Data Protection Policy and Privacy Notice** should be read in conjunction with the overarching [University of Kent Data Protection Policy](#).

Throughout the **HEAT Service Data Protection Policy and Privacy Notice** all references to Data Controller, Data Processor, Data Subject, shall have the same meaning as in the Data Protection Act 1998, Data Protection Act 2018 (UK implementation of the General Data Protection Regulation 2018), and any subsequent prevailing data protection legislation. In so much that the **HEAT Service**:

- a. processes data to generate reports both independently and on behalf of member institutions,
- b. holds personal data on behalf of member institutions, enabling them to produce reports and undertake their own analysis,

the **University of Kent (HEAT Service)** is determined under the Data Protection Act and General Data Protection Regulation to be both Data Controller and Data Processor, for aspects of its activities.

What is the HEAT Service and what does it do?

Led by the **University of Kent**, the **Higher Education Access Tracker (HEAT)** is a not for profit, monitoring and evaluation service funded through an equal subscription model, strategically governed by its members. Initially grant funded by the Higher Education Funding Council for England (HEFCE), the service will become entirely 'self-sustaining' with effect from 1st January 2018.

Membership of the HEAT service is currently available to Higher Education institutions (HEIs) in England, and carefully selected non-HE organisations (e.g. education providers or third sector agencies). Subscribing members have access to the HEAT Database, a secure online platform which enables data collection, analysis and research via standardised and bespoke reporting functionality.

What is HEAT's purpose (lawful basis) for collecting data?

Article 6 of the GDPR requires Data Controllers to have a lawful basis in order to hold and process personal data. The GDPR expands current Privacy Notice requirements based on the widened first principle, which now specifically requires controllers to be transparent about their processing. Examples of lawful bases under the GDPR (called schedule conditions under the DPA) include:

- **Necessary for a contract**
- **Necessary to comply with a legal obligation**

- **Necessary in the legitimate interest of the business**
- **Necessary for a task carried out in the public interest**

Under UK derogations to the GDPR, universities will be classified as Public Authorities in the fullest sense of the term. Although the overarching function is primarily to educate, universities are also statutorily required to demonstrate financial integrity and performance accountability, particularly relating to educational outcomes, therefore certain university activities are deemed to be tasks necessarily carried out 'in the public interest'.

The HEAT Service enables members to monitor and evaluate Widening Participation and Outreach programmes longitudinally; tracking the progression of participating students to investigate the impact of Widening Participation and Outreach on their attainment, progression, social mobility, graduate outcomes and eventual employment.

The lawful basis of **a task carried out in the public interest** is therefore applicable to data collected and processed by the **HEAT Service** on behalf of HEAT member universities, in terms of enabling them to meet their statutory obligation to evidence effectiveness of such programmes to funders, education regulators such as (but not limited to) the Office for Students, and central Government.

What data is collected and from where?

HEAT member universities and organisations are Data Controllers in their own right, and accordingly have their own organisational Data Protection Policies, one of a range of stringent and legally binding requirements for membership of the HEAT Service. These membership requirements are described in **Compliance requirements and minimum standards for HEAT member institutions**.

HEAT members collect student data, either directly from participants in their Widening Participation and Outreach programmes, or indirectly from partner schools, colleges and other agencies with whom they collaborate for programme delivery. Individual Data Controllers have a legal obligation to provide, or direct data subjects to, their own mandatory Data Protection Policy and Privacy Notice, together with their Data Controller contact details, and information on the rights of data subjects.

These mandatory documents, provided by individual Data Controllers (HEAT members) must be completely transparent and explicit about when data is collected; what is collected; why it is collected; how it will be held, analysed or used (the lawful basis); who it will be shared with and how long data will be retained. A Data Controller must also indicate when profiling or automated decision making activities take place, providing justification that the profiling is compatible with its lawful basis.

How does HEAT process and use the data?

The HEAT Service provides a secure, central online repository within which HEAT member institutions and organisations store student data, in order to facilitate monitoring, evaluation and evidence based research. See also **HEAT's purpose (lawful basis) for collecting the data**.

The HEAT database produces standardised or personalised data collection and reporting for members, using bespoke tools to facilitate reporting on students and/or activities, including:

- Secure and confidential recording of individual students and their participation activities
- Import and exports to ease data capture and outputs
- Data sharing functionality across partner institutions and organisations (where formal data sharing agreements and protocols are in place)
- Postcode profiling
- HEAT Track

The HEAT Track enables tracking of individual students through the outreach process and, subject to appropriate consent, linking both participant and student outcome data through administrative data sets from the Department for Education, Skills Funding Agency and the Higher Education Statistics Agency, to explore in detail the relationship between outreach participation and student success.

Profiling

Student profiling is central to HEAT's analysis and reporting. Widening Participation policies are intended to help certain groups of students, thus students added to the HEAT central database are profiled to assess the extent to which they belong to these target groups. This serves two fundamental purposes, which are:

- to allow HEAT to monitor whether resource has been targeted effectively
- when conducting evaluation analyses, HEAT is able to assess the impact on those for whom widening participation and fair access policies were intended

It is important to clarify that HEAT's profiling activity is used solely for the analysis and reporting purposes described above, and is NOT linked to or used for any decision making process which might directly affect individual students.

Who is profiled data shared with?

Reporting and analysis based on profiled data are provided to HEAT members in aggregate tables, without disclosing the characteristics of individual students. Profiled student level data are, in some cases, available to HEAT members, depending on the source of the data.

The table below summarises the characteristics on which students are profiled, and indicates which are available to members and which may be accessed through the postcode profiler tool.

Students are profiled based on the following characteristics:

Characteristics	Based on	Source	Accessed through postcode profiler tool	Student level data shared with HEAT member
POLAR Quintile	Student postcode	HEFCE	Yes	Yes
Index of Multiple Deprivation	Student postcode	MHCLG	Yes	Yes
Income Deprivation Affecting Children Index	Student postcode	MHCLG	Yes	Yes
Education Skills and Training Index	Student postcode	MHCLG	Yes	Yes
Acorn Group	Student postcode	CACI	Yes*	Yes*
Free School Meal Eligibility	Student NPD record	NPD	No	No
First generation HE	Student survey	HEAT	No	Yes (collected by HEAT member)
Gender	Student survey	HEAT	No	Yes (collected by HEAT member)
Ethnic Group	Student survey	HEAT	No	Yes (collected by HEAT member)

*License with CACI required

How long do we keep the data?

The GDPR data protection principles set out the main responsibilities for organisations. Article 5 (1) pertains directly to personal data and requires that it will be:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes
- c) adequate, relevant and limited to what is necessary in relation to the legitimate purposes
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay

- e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
- f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

The **HEAT Service** is committed to demonstrating compliance with data retention requirements of the GDPR, whilst also prioritising the fundamental ethos and longitudinal research purposes of HEAT. The two are not mutually exclusive, thus with carefully considered application of the research provisions contained in Article 5 (1) sections b, e and f of the GDPR Principles, and adherence to relevant University of Kent policies (eg; [Records Management Policy](#), [Document Retention and Archiving Policy](#)) both essential areas can be addressed effectively and compliantly.

The **HEAT Data Retention Schedule** comprises the HEAT membership's Research Aims, overall rationale, schedule of data retention, and data anonymisation protocols. The schedule has been scrutinised by the ICO and their recommendations duly incorporated, before final ratification by the HEAT Steering and Governance Groups. In accordance with its accountability and governance commitment, (described in [Internal procedures and protocols, section a\) Accountability and Governance](#)), the Data Retention Schedule will be subject to a regular schedule of internal review, so as to ensure it remains fit for purpose and compliant with relevant legislation.

Who to contact about subject access and rights, make an enquiry, or complain if you are unhappy

Freedom of Information requests, Subject Access Requests, Data Subject Rights, or any data protection enquiries pertaining to the business of the **University of Kent**, should be made to the university's Data Protection Officer by email, to datapro@kent.ac.uk

For further data protection information, advice and guidance, or to make a complaint you should contact the regulatory body for data protection in the United Kingdom, the **Information Commissioner's Office (ICO)**. The ICO is the UK's independent regulatory body set up to uphold information rights in the public interest.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Website: www.ico.org.uk

Telephone helpline: **0303 123 1113**