Data Protection Policy & Privacy Notice

1. Data Protection Policy

Context and Scope

Under the Data Protection Act (DPA) 1998, and the General Data Protection Regulation (GDPR) 2018, we (The **University of Kent** and the **HEAT Service**) have a legal duty to safeguard personal data collected and processed for the legitimate purposes of the HEAT Service, and to exercise fully our responsibility in respect to the rights, freedoms and privacy of those individuals whose data we hold.

The **University of Kent** is registered on the **Information Commissioner's Office** (ICO) **Data Protection Register**, number **Z6847902**, and information included in this policy and associated documentation is based on guidance and codes of practice provided by the ICO.

Managed and led by the **University of Kent**, the **HEAT Service** adheres to and complies with the **University of Kent, Data Protection Act 1998, Code of Practice** (otherwise referred to as the **University of Kent Data Protection Policy)**, which can be accessed here: *University of Kent Data Protection Policy*. The policy demonstrates the University of Kent's compliance with the provisions of the Data Protection Act, in particular the underpinning Data Protection Principles which require that personal data:

Principle 1: shall be processed fairly and lawfully

Principle 2: shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or purposes

Principle 3: shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

Principle 4: shall be accurate and, where necessary, kept up to date

Principle 5: shall not be kept for longer than is necessary for the stated purpose or purposes

Principle 6: shall be processed in accordance with the rights of data subjects under the Act

Principle 7: shall be safeguarded and protected against unauthorised or unlawful processing, and against accidental loss or destruction of, or damage to personal data by the implementation of appropriate organisational and technical measures

Principle 8: 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

Complete definitions of the Principles are contained in the *University of Kent Data Protection Policy*.

2. 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 (DPA) 1998, the General Data Protection Regulation (GDPR) 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.

3. Data Protection and Privacy Procedures

Compliance requirements and minimum standards for HEAT member institutions

Whilst recognising that HEAT member institutions and organisations have individual, legal accountability as Data Controllers, the **HEAT Service** remains committed to an ethos of 'due diligence', promoting and upholding compliance with Data Protection legislation across the HEAT membership as far and in so much as that is reasonably possible and practicable. Membership of the HEAT service is dependent upon participating universities and organisations entering into a legal agreement with the **University of Kent (HEAT Service)**, which governs delivery, access and use of the HEAT Service.

The **HEAT Service Member Agreement** details the mutually contractual obligations and legal accountabilities of the parties, alongside an expectation of minimum compliance standards. Explicit requirements include (but are not limited to) Confidentiality, Data Protection, Data Sharing Protocols and Safeguards, Governing Law, Intellectual Property, Liability, and pursuant to its commitment to compliant practice, the **HEAT Service** requires members to append documentary evidence of its own organisational policies and safeguards to the **HEAT Service Member Agreement**.

Information collected from HEAT Members

In order to administer the **HEAT Service Member Agreement** contract, HEAT necessarily collects and retains business contact information from service users and authorised representatives of member universities. This may include name, telephone number, email address and job title information, which is used by the HEAT Service solely to create and maintain user accounts for the HEAT Database, and provide communications and updates relevant to the delivery of the HEAT Service. HEAT does not use this information for any other purpose and does not disclose contact information to third parties.

Other Information

Our servers automatically collect all access and usage information for the HEAT Database, recording it in audit log files. Collection and processing of this log data is necessary to:

- monitor system functionality and maintain service levels
- identify and respond to technical issues or malfunctions
- ensure integrity and security of the database
- detect and prevent system abuse and unauthorised access
- monitor and maintain access restrictions and protocols
- evidence our commitment to technological security

Information collected from prospective HEAT members and other enquirers

In the **Legitimate Interest** of administering to HEAT Service enquiries, contact information will be retained for the sole purpose of communicating the requested or subsequent information. HEAT does not use the contact information for any other purpose and does not disclose it to any third parties.

HEAT internal procedures and protocols

The **HEAT Service** is committed to meeting its responsibilities as both Data Controller and Processor, by upholding the security of personal data, and protecting the rights and freedoms of data subjects. In order to demonstrate and evidence accountability, Article 5(2), we have in place:

- comprehensive strategic governance
- robust technological and organisational measures
- security procedures to minimise the risk of unauthorised access or disclosure

- documented records of processing and profiling activities
- information audit and data protection risk assessment procedures
- staff training and associated safeguards
- legally binding third party agreements for consultants and contractors

a. Accountability and Governance

All **HEAT Service** operations and procedures are subject to a regular schedule of internal review and scrutiny, by both the HEAT Steering Group and HEAT Governance Board. See also **HEAT internal procedures and protocols**, section g) Changes to our Privacy Policy and Procedures

b. Data Protection by design and default

The **HEAT Service Privacy by Design and Default** strategy seeks to demonstrate a 'due diligence' approach to privacy and data protection across its technological activities, and evidence compliance with the new Privacy by Design and Default mandatory obligation. GDPR Article 25 describes that:

"The data controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility".

The internationally recognised **Privacy by Design** framework (developed by the IPC for Ontario, circa 1990 and now incorporated into the GDPR), is identified by the ICO as a significant tool to assist organisations in developing a compliant approach, and that the foundation principles of the framework *"will be relevant for UK data controllers".*

The **HEAT Service Privacy by Design and Default** strategy is therefore be informed by the IPC (Ontario) **Privacy by Design** framework, the GDPR Article 25 requirements, and any current and future guidelines issued by the ICO.

HEAT aims to achieve the objectives of **Privacy by Design** by embedding the 7 foundation principles of the framework into all project planning and development activities, and everyday practice:

- **Proactive** not reactive measures: anticipating and aiming to prevent invasive events from occurring rather than waiting for them to materialise
- Privacy as the **Default Setting**: personal data is automatically protected to the highest level in any given IT system or business practice
- Privacy **Embedded** in design: not bolted on as an 'add-on' after the fact, but incorporated into the design and architecture of IT systems so that privacy becomes an integral and essential component of the core functionality

- Full functionality – **Win-Win**: not a conflict between privacy vs. design, but a framework within which legitimate business interests and the requirement for privacy are both possible
- **End to end security**: Privacy by Design means secure, entire lifecycle management of the data involved, not just embedding into the system at development or implementation stages
- **Visibility and Transparency**: assurance to data subjects that whatever the technology, their data is processed entirely in accordance with the legitimate purpose and stated objectives
- **Respect** for user privacy: developers, controllers, processors and users are all required to protect the privacy, rights and freedoms of individuals by applying measures such as robust privacy and security defaults, explicit information, and fair and lawful processing of data

c. Organisational and technical measures

When determining what measures to put in place, **HEAT** will be permitted to take into account:

- the state of the art
- the cost of implementation
- the nature, scope, context and purposes of processing
- the varying likelihood and severity of risk to the rights and freedoms of natural persons posed by the processing

In terms of minimising the risk of unauthorised access or disclosure, and demonstrating GDPR compliance, **HEAT** will implement appropriate technical measures such as:

- pseudonymisation / anonymisation / data minimisation
- privacy enhancing technologies (e.g. encryption)
- storage limitation and retention schedules
- access restrictions and protocols
- data sharing and secure data transfer protocols
- IT infrastructure security – routine back-ups; anti-virus, firewalls and other protections, timely application or security updates, stringent testing regimes
- organisational measures including (but not limited to):
    - information audit and data protection risk assessment procedures
    - documented records of processing and profiling activities
    - policies, procedures, protocols
    - staff training and associated safeguards

- legally binding third party agreements for consultants and contractors

d. Data Protection Information Audits and Privacy Impact Assessments

As a service holding and processing large scale, national level data of significant numbers of individuals, the **HEAT Service** acknowledges its responsibility to undertake appropriate Information Audits and Data Protection Impact Assessments (DPIA), so as to inform its Data Protection Policy and Procedures.

The DPIA and PIA processes will be used by the **HEAT Service** to:

- Describe its processing operations and purpose, ie; the lawful basis for processing
- Monitor the necessity and proportionality of the processing in relation to the purpose
- Identify and assess potential risks to the rights and freedoms of data subjects
- Inform necessary measures to mitigate risk, including security, and to demonstrate compliance

e. Staff training and personnel security

All **HEAT Service** staff undertake mandatory data protection awareness training through the **University of Kent** staff training programme, with supplementary training specific to the requirements of their individual roles. In addition to data protection training, staff in roles requiring the highest levels of data access (ie; Technical Development, Support, Data Analysis, Strategic Management), will be subject to an enhanced check with the **Disclosure and Barring Service**.

f. Contractor and Consultancy (Third Party) Agreements

Where the **University of Kent** and/or the **HEAT Service** decide to use an external organisation or consultant to (for example):

- handle, process, cleanse or analyse personal data on our behalf
- host or maintain systems
- develop, test or in any other way work on or have access to systems
- undertake specific contracted projects or areas of work using personal data

it retains legal responsibility for ensuring security of the data and protecting the rights and freedoms of data subjects. In deciding appropriate security measures, the type of data, level of risk, available technology and the cost of ensuring data security, will be fundamental priorities.

Contractual arrangements with external organisations or consultants by the **HEAT Service** are subject to extensive, legally binding Third Party Agreements, which seek to ensure appropriate security measures in addition to compliance with the requirements of the Data Protection Act (DPA) 1998 and General Data Protection Regulation (GDPR) 2018. Accordingly the **HEAT Service,** in conjunction with the **University of Kent,** will take all reasonable precautions when outsourcing

services, to select reputable organisations and consultants, utilising the expertise and guidance of the University of Kent's **Information Compliance Officer** and **Information Services Requirements Team** as appropriate.

g. Changes to our Privacy Policy and Procedures

The **HEAT Service Data Protection Policy and Privacy Notice** and associated procedures, are reviewed and ratified annually by the HEAT Governance Board in accordance with relevant guidelines.

Additional expertise, advice and scrutiny will be sought where necessary from the **University of Kent, Data Protection Officer,** and/or the **Information Commissioner's Office.**

As a service led by the **University of Kent**, the **HEAT Service** operates at all times under the *University of Kent Data Protection Policy*, therefore any revisions or updates to this document will be in accordance with the University of Kent policy review schedule.

4. Data subject access and rights

The GDPR provides the following rights for data subjects:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

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 Data Protection Officer
Information Governance Team
The Registry
University of Kent

Canterbury
Kent CT2 7NZ

Email: datapro@kent.ac.uk

Telephone: **01227 823671**

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**