Data Protection Policy

1. Introduction

1.1 The University of Kent collects, processes and retains data in order to deliver its operational and strategic objectives and to support its business functions. The University takes its responsibilities around Data Protection seriously and as such it is committed to meeting its legal obligations in respect to the processing of personal data.

1.2 The purpose of this policy is to clearly set out the responsibilities of the University as Data Controller under the Data Protection Act 2018 (DPA 2018), the General Data Protection Regulation (GDPR) and any associated legislation, through the establishment of an effective compliance framework.

1.3 This document also sets out a series of policy principles which are designed to underpin procedures and controls that serve to create and maintain a robust Information Governance System.

1.4 All staff, students and any other users of University data must comply with this Policy. Disciplinary action can be taken against those who do not comply, particularly in cases when there has been deliberate, wilful or negligent disregard of the Policy and other University requirements.

2. Definition of Personal Data

2.1 For the purposes of this policy, 'personal data' is defined as information relating to natural persons who

- can be identified or who are identifiable, directly from the information in question; or
- can be indirectly identified from that information in combination with other information.

3. General Principles

3.1 The University of Kent shall ensure that the following principles are met when processing personal data:

- that we process personal data lawfully, fairly and in a transparent manner;
- that we ensure that personal data is 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;

University of Kent

- that the personal data held by the University is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- that any personal data held by the University is accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- that such data is 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
- we ensure that personal data is 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.

4. The University of Kent as Data Controller

4.1 The University of Kent is registered as a Data Controller with the Information Commissioner's Office (registration number Z6847902).

4.2 As a registered Data Controller, the university is legally responsible for determining the purposes for which, and the manner in which any personal data are or are to be processed.

4.3 There may be occasion when the University of Kent acts as a joint Data Controller with another party or be considered a Controller in common with another party. In such circumstances all such controllers shall enter into a formal agreement that sets out the duties and obligations each party owes to each other and to data subjects in regards to the processing of personal data.

5. The Data Protection Officer and their responsibilities

5.1 The University of Kent is a public body and therefore must appoint a Data Protection Officer (DPO).

5.2 The Head of Data Protection shall be the University of Kent's designated DPO and shall fulfil the statutory duties associated with that role.

5.3 The University must ensure that the DPO is sufficiently independent from any processing activities so as to ensure that there are no conflicts of interest in the exercise of their duties.

5.4 The DPO shall be responsible for the monitoring of organisational compliance with data protection legislation, this may be done through audits and reviews.

5.5 The DPO will inform and advise the University on matters relating to data protection, legislative compliance around the holding and processing of data and promote awareness of good information governance practices.

5.6 In order for the DPO to exercise these responsibilities, they shall have access to adequate resources provided by the University and will have direct reporting access to the University's senior management.

5.7 The DPO shall act as the University's main point of contact with the ICO and assist the ICO in their work with the university. Staff should reasonably assist the DPO in the exercise of their duties.

5.8 The DPO shall make regular reports on these activities to the Executive Group of the University as well as to other relevant governance committees as required.

6. Processing Data in a Lawful, Fair and Transparent Manner

6.1 When collecting and processing personal data, the university shall ensure that it meets one of the following lawful conditions of processing:

- Consent: where an individual has given clear consent for the University to process their personal data for a specific purpose.
- Contract: the processing is necessary for a contract the University has with an individual, or because an individual has asked the University to take specific steps before entering into a contract.
- Legal obligation: the processing is necessary for the University to comply with the law (not including contractual obligations).
- Vital interests: the processing is necessary to protect someone's life.
- Public task: the processing is necessary for the University to perform a task in the public interest or for one of the University's official functions, and the task or function has a clear basis in law.
- Legitimate interests: the processing is necessary for legitimate interests of the University or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (The University shall not rely on this condition when processing is necessary for the performance of our public tasks).

6.2 The University of Kent shall only process special category data if the provisions contained in Article 9 GDPR are met. The Information Compliance Office shall provide advice on the processing of special category data to the University.

6.3 The University shall ensure that all personal data held under its control is collected and subsequently processed for a defined purpose, that the data is adequate for the fulfilment of that purpose and limited to that which is necessary to achieve that purpose. The University shall ensure that the data is accurate and kept up to date.

6.4 The University shall process personal data in a transparent and accountable manner and shall ensure that data subjects are provided with privacy information that is concise, transparent, intelligible and easily accessible. Data subjects shall be provided with this information at the time of collection if obtained directly from the individual. If personal data is obtained from other sources the data subject shall be provided this information within one month of the commencement of processing or at the first point of communication. The University shall maintain this information in the form of privacy notices on publically accessible webpages, which shall be kept up to date.

6.5 The University shall maintain an Information Asset Register that shall serve as the University's Record of Processing Activities. The IAR shall be regularly reviewed to ensure that it remains accurate and up to date.

7. Transfers of Personal Data outside the EEA

7.1 The University shall not transfer data to an entity based outside of the EU unless the transfer is subject to appropriate safeguards.

7.2 These safeguards include the use of the EC's Standard Data Protection Contractual Clauses where a state has not received an adequacy decision.

8. Data Protection by Design and Default

8.1 The University is committed to embedding a culture of Data Protection by Design and default across the organisation.

8.2 When the University is considering a change to any of the existing processing tasks as detailed in the Information Asset Register, or is considering designing and implementing a new data processing activity, it shall ensure that the principle of 'data protection by design and default' is a central consideration in any of the associated development work.

8.3 Staff members considering changing the nature of existing processing activities or devising new processing activities must first contact the DPO to discuss their intended purpose.

8.4 The DPO shall work collaboratively with key stakeholders to identify, manage and mitigate data protection and information security risks.

8.5 Where the amended or new process is likely to result in a high risk to the rights and freedoms of natural persons, the DPO will require the Information Asset Owner or their representative to complete a Data Protection Impact Assessment.

8.6 Where the University decides to not comply with the advice of the DPO, this shall be recorded and reported to the Executive Group and the University's Risk Officer for inclusion in the University's risk management plan.

8.7 Personal data collected as part of academic research is subject to the General Data protection Regulation. The University shall ensure that data protection issues and risks are addressed during the ethics approval process.

9. Security of processing

9.1 The University of Kent shall maintain an Information Security Policy as well as establish and maintain appropriate technical and organisational measures to ensure the security of data under its control, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

9.2 The University of Kent shall have mechanisms in place to test the effectiveness of these measures, addressing any identified weakness in controls and actively implement any necessary mitigation for perceived risk.

9.3 Where the University of Kent has engaged a third party as a data processor or is jointly working with another Data Controller, the University shall conduct due diligence checks on the third party's information security levels and GDPR compliance before transferring any personal data to that party.

10. Personal Data Breaches

10.1 The University shall establish, maintain and promote a Data Breach Policy.

10.2 The policy shall provide the basis for implementing appropriate procedures to ensure that the Data Breach policy is effective in the recording and management of any potential breaches of personal data under the control of the University.

10.3 The same procedures shall apply to breaches relating to personal data which the University is processing on another Data Controller's behalf.

11. Information Rights

11.1 The University of Kent shall have a Data Rights Policy which shall provide a framework for its response to data subject rights requests exercised under the provisions made in the GDPR and DPA 2018.

12. Sharing Personal Data with Third parties

12.1 Where the University of Kent has engaged a third party to deliver services under contract and the delivery of those services requires the processing of personal data, the University shall require the third party to sign a data processing agreement or to include adequate data protection clauses within the principle contract.

12.2 Where the University of Kent is working in partnership or collaboration with another Data Controller, the University shall establish their obligations and respective duties to each party in a formal data sharing agreement.

12.3 The Information Compliance Office shall assist colleagues in the preparation of these agreements and advise on the status of the University of Kent in respect of the personal data processed under those agreements.

12.4 The Information Compliance Office shall regularly check that the agreements that exist are properly followed.

12.5 From time to time the University may receive requests to disclose personal data to external parties. In all circumstances the external party must provide their lawful reasons for requesting the data. The Information Compliance Office shall consider the circumstances of each request and determine the degree to which data can be lawfully disclosed.

13. Data Retention

13.1 The University of Kent will have a Records Management Policy which will outline the University's approach to the management of records under its control.

13.2 The retention periods for each type of data shall be appended as a schedule to the Records Management Policy.

13.3 Retention periods shall be determined by balancing business aims and regulatory obligations against privacy rights.

13.4 The University of Kent shall ensure that the retention schedules are followed by conducting regular reviews of compliance and shall review retention periods so as to ensure that they align with best practice. This work will be closely aligned to the University's activities in maintaining the IAR.

14. Training and Awareness

14.1 Data Protection training shall be mandatory for all staff. Existing staff shall complete refresher data protection training every two years.

14.2 All new staff shall complete Data Protection training as part of their probation.

14.3 The DPO shall regularly monitor the completion rates for staff members and report completion rates as part of their regular reports to senior management

14.4 The DPO shall, in conjunction with other stakeholders, implement a communication and awareness plan which shall champion data protection best practice, disseminate information Security updates and reinforce the value of good Information Governance.

15. Staff Responsibilities

15.1 Serious breaches by staff of this policy caused by deliberate, negligent or reckless behaviour may result in action being taken in accordance with Ordinance 39: Conduct and may even give rise to criminal offences.

Document review date

This policy will be reviewed annually by the Data Protection Officer.

Policy created: 2nd March 2020

Policy reviewed: review by 2nd March 2021