Somerville College

Data Retention Policy

1. Principles of Data Retention

Somerville College is committed to the efficient management of our records. This is necessary

- for the effective delivery of our services
- to document our principle activities
- to maintain the institutional memory
- to communicate with college members

We will only keep records that enable us to fulfil these functions and we will dispose of data in a secure manner, once no longer needed.

Information held for longer than is necessary carries additional risk and cost. Under GDPR and the DPA 2018, personal data processed by the college must not be retained for longer than is necessary for its lawful purpose. However, personal data may be stored for longer periods insofar as it will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of GDPR. The College's lawful bases for processing different types of personal data are set out in our Privacy Notices.

The Policy applies to all documents, both electronic and paper, produced by the college or any of its third party contractors and held in College systems, which contain data relating to the College's activities. It covers personal data held in a variety of formats including CCTV, images, emails, electronic documents and paper files. The policy is intended primarily as a resource for those responsible for processing data and to ensure the disposal of records is carried out in a consistent and controlled manner.

2. Responsibilities

- Retention periods are set by the various departments within the college in consultation with the Data Protection team and consolidated in a Data Retention Schedule held by the Data Protection team.
- Once retention periods have been set, all staff are responsible for managing, storing appropriately and disposing of the information they create and receive as part of their normal business activities.
- Heads of Departments hold ultimate responsibility for ensuring compliance with the policy and will use automated methods of destruction wherever possible in consultation with the ICT department.

Retention periods will be reviewed periodically and any changes to be made to the schedule should be agreed by the relevant Head of Department in consultation with the DP team.

3. Retention Periods and Procedures

The College collects, processes and stores various different categories of data. Each category has its own retention period which applies to all records in that category and to all formats. Data retention periods will be set by the Heads of Departments in consultation with industry regulations or best practice, university recommendations and the data protection team. The data retention period should be adhered to wherever possible, although it is recognised that there may be exceptional circumstances which require documents to be kept for either shorter or longer periods. If individual records or documents require an alternative retention period, this must be agreed with the Data Protection team in advance of any change and a record of the reasons for the change retained.

A schedule detailing all the different types of data processed by the college including their retention periods is maintained by the Data Protection team and updated on an annual basis. Detailed procedures for reviewing, archiving and securely destroying data are maintained within each department and centrally with the Data Protection Team.

Any challenges to the retention of personal data must be considered in accordance with GDPR Article 17 (Right to erasure), or the equivalent sections in the DPA 2018 if the processing is for law enforcement purposes. The right to erasure does not apply where we are legally obliged to process personal data or where the processing is necessary for performing our functions.

Once data is due for destruction it will be deleted from shared drives and accounts, securely shredded or otherwise permanently and securely destroyed, including , where applicable, data held by third parties.

4. Audit and compliance

Data Protection processes, including retention and destruction of data, are audited periodically by the Data Protection Team. A report on data protection activities is produced quarterly by our DPO. Individuals who are found to be non-compliant with this policy may be subject to disciplinary procedures.

5. Policy review

This Policy will be reviewed annually by the IT Committee and any amendments approved by Governing Body.

AM January 2019

KOD February 2019

AM June 2019