Retention and Disposition Policy

Written by:	Quality and Compliance Manager
CLT Sponsor:	Richard Church
Consulted with:	Chief Financial Officer, Director of Finance, Funding and MIS, ICT Manager
Next Review Date:	February 2023
Version:	February 2021

1 Purpose and Scope

The storage limitation Principle of the UK GDPR provides that personal data shall not be kept for longer than is necessary for the proposes of processing. There are no interpretative provisions in the UK GDPR that relate to this Principle per se, and there are no set periods of time to which controllers must adhere. Exeter College is therefore required to determine an appropriate retention period, having regard to the purposes for which this information and data was collected. This Retention and Disposition Policy needs to be read and understood in connection with other relevant policies and documentation set out under point 5.

This Retention and Disposition Policy:

1.1 sets out the minimum standards to be applied for the retention and disposal of information and personal data.

1.2 applies to all business units, processes and systems across all departments and faculties of Exeter College and all subsidiary companies.

1.3 applies to all staff at Exeter College who have access to data (including personal data and/ or sensitive personal data).

1.4 applies to all information used at Exeter College. Examples of documents include, but are not limited to:
- 1.4.1 Emails
- 1.4.2 Hard copy documents
- 1.4.3 Electronic copy documents
- 1.4.4 Video
- 1.4.5 Audio

2 Definitions

2.1 Exeter College – Exeter College and all subsidiary companies
2.2 SIRO – Senior Information Risk Owner. The College's SIRO is the Assistant Principal for Quality and Student Experience. The SIRO is accountable for the information risk across Exeter College and for sponsoring and promoting policies connected with Information Governance.
2.3 IAO – Information Asset Owners are accountable for ensuring their information assets are identified and compliant with all subsidiary policies and legislation.
2.4 DPO – Data Protection Officer. The College's DPO is the Quality and Compliance Manager.
2.5 SDG – Systems Development Group
2.6 GDPR – General Data Protection Regulation

3 Policy

3.1 Retention

3.1.1 Exeter College will maintain its information assets for an appropriate time, considering its legal, regulatory, fiscal, operational, and historical requirements.

3.1.2 Subject to the provisions of the Exception Schedule, Exeter College will retain personal data, including special categories data, for a period of 7 years following the ending of its formal relationship with the data subject. Within 1 year of the 7th anniversary, personal data will be anonymised, deleted or securely destroyed.

3.1.3 The time period for which documents and electronic records should be retained is defined in the Data Retention Schedule. The Data Retention Exception Schedule lists all permissible exceptions to the 7-year

standard. Exceptions may be determined by legal, contractual, business or subject rights requirements. The Schedule will be reviewed annually by the DPO and amendments proposed and authorised by the Systems Development Group. It will form part of the privacy information provided to data subjects and will be made available on the Data Protection and Privacy section of the college website.

3.1.4 As an exemption, retention periods with the Data Retention Schedule can be prolonged:

- if there is an ongoing investigation from authorities (e.g. the ICO)
- if personal data are needed by Exeter College to prove compliance with any legal requirement
- if there are ongoing legal proceedings

3.2 Destruction of Data

3.2.1 Exeter College and its employees will review all data on a regular basis, whether held electronically or on device or on paper, to decide whether to destroy or delete any data once the purpose for which such data was created is no longer relevant.

3.2.2 The overall responsibility for the destruction of data falls to the SIRO and the IAOs, with the support and advice of the DPO.

3.2.3 Once the decision is made to dispose according to the Data Retention Schedule, the data should be deleted, shredded or otherwise destroyed depending on the level of confidentiality. The method of disposal will vary and depend on the nature of the document to be destroyed:

- documents that contain personal data, sensitive or confidential information and sensitive personal data, will be disposed of as confidential waste and be subject to secure electronic deletion
- destruction of electronic records should ensure that they are non-recoverable even when using forensic data recovery techniques
- expired or outdated documentation that does not contain personal data, sensitive or confidential information may be disposed of using recycling bins

4 Implementation

4.1 Roles and responsibilities

4.1.1 The SIRO is responsible for the oversight of this policy. The SIRO will be accountable to the Board regarding all relevant matters and support the DPO and all IAOs in ensuring that Exeter College's approach to retention and disposition of data and information is in line with this and all related policies.

4.1.2 The DPO is responsible for the maintenance and operation of the policy and will support and advise IAOs and employees at Exeter College who are charged with retaining or destroying information and personal data.

4.1.3 The ICT Manager will support and advise the DPO and IAOs in relation to electronically held data and information with regard to its secure destruction.

4.1.4 The Systems Development Group will propose and authorise relevant changes to the Data Retention Schedule and the Data Retention Exception Schedule.

4.1.5 IAOs, where they are Heads of Department and Faculties, are responsible for ensuring that retention and disposition of data and information is in line with this and all related policies.

4.1.6 All employees will ensure they understand and comply with procedures in support of this and related policies to ensure information and personal data is retained and destroyed securely and, where relevant, in compliance with the law.

4.2 Procedure relating to the retention and disposition of data

4.2.1 The SIRO, with the support of the SLT, shall decide on the timeframe for regular disposal of personal data, where it is inappropriate for IAOs across the college to take such decisions independently.

4.2.2 The DPO, after discussion with and instruction from the SIRO, will support IAOs with advice and guidance on procedures to support this policy.

4.2.3 The ICT Manager will support with updates on electronic back-ups of personal data and work together with the SIRO and the DPO to ensure compliance with the UK GDPR.

5 Associated Documentation

5.1 Data Protection Policy
5.2 Information Governance Policy
5.3 The Data Retention Schedule
5.4 Information Security Policy
5.5 Data Loss Response Procedure
5.6 UK GDPR
5.7 General Data Protection Regulation Keeling Schedule

6 Monitoring, Review and Evaluation

6.1 The Senior Leadership team is responsible for the approving of the Retention and Disposition Policy

6.2 The Board (Business Services Committee) is responsible for adopting the Retention and Disposition Policy

6.3 The Data Protection Officer is responsible for the maintenance, review and monitoring of the Retention and Disposition Policy and will conduct a bi-annual review of the policy and an annual review of the related Data Retention Schedule.

6.4 The definitive version of this policy is stored in the College Leadership SharePoint Site