# 大连海事大学文件

连海大校发〔2022〕291号

## 大连海事大学关于印发《大连海事大学数据管理办法》的通知

各单位（部门）：

《大连海事大学数据管理办法》已经2022年第42次党委常委会会议审议通过，现予以印发，请遵照执行。

特此通知。

大连海事大学

2022年12月1日

# 大连海事大学数据管理办法

## 第一章　总　则

**第一条** 为规范大连海事大学数据处理活动，推动互联互通和数据共享，保护学校、个人的合法权益，保障数据安全，根据《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规以及国家有关政策标准的要求，结合学校实际情况，制定本办法。

**第二条** 本办法所称数据是学校各单位（部门）和全校师生在履行职责过程中产生、获取和累积的，以及按上级部门要求报送的各类报表和日常工作中各类统计分析报告等非涉密信息，是任何以电子或者其他方式对信息的记录。

**第三条** 本办法适用于学校数据处理活动及其安全监管，数据处理，包括数据的收集、存储、使用、加工、传输、提供、公开等。

**第四条** 数据管理应遵循以下原则:

**（一）统筹推进。**遵循“一数一源”，编制数据资产目录体系，统筹建设数据平台，统筹推进数据持续动态治理。

**（二）开放共享。**以共享为原则，不共享为例外，建立健全数据开放共享机制。

**（三）分类分级。**建立数据分类分级管理制度，对列入目录的数据进行重点保护。

**（四）安全可控。**建立数据备份、日志记录等保障机制，数据处理遵循“最小必要”、“最短周期”等原则。

## 第二章　组织与职责

**第五条** 数据管理部门是信息化部门，负责制定标准规范，编制数据目录，推动数据治理，实现互联互通、开放共享。

**第六条** 数据责任部门是数据源部门，负责收集本业务领域产生的数据，并保障数据质量。

**第七条** 数据使用部门是有数据共享需求的部门，可通过数据平台申请获取数据的使用权。

## 第三章　数据处理

**第八条** 按照“一数一源、最小必要”原则，数据责任部门利用业务系统收集本业务领域产生的数据，其他部门不得重复收集。当业务系统不满足收集条件时，可会同数据管理部门通过数据平台收集，或采取“大平台+微服务”模式新建业务应用的方式收集，原则上不得线下收集。

**第九条** 制定数据存储传输、备份恢复的安全策略，数据存储遵循“最短周期”原则，重要数据应在校内存储，并采用密码

技术保障数据存储和传输安全。

**第十条** 数据责任部门明确相应的数据管理员，授权其负责数据质量，确保数据的准确性、完整性、规范性和时效性。

**第十一条** 数据管理部门编制数据资产目录，标记数据关系，构建血缘关系，数据目录向全校公开并动态更新完善，推动数据互联互通、开放共享。

**第十二条** 建立数据共享审核机制，数据使用部门查阅数据资产目录，利用数据平台按照“最小必要”原则向数据管理部门提出共享申请，鼓励通过数据接口方式共享数据，不得以离线文档形式传递。数据共享实行审批制。

## 第四章　数据治理

**第十三条** 数据管理部门负责搭建数据平台，制定流程规范，建立数据展示、纠错、共享和监测机制，提供数据质量报告、纠错监控、临时数据维护等功能，持续推动数据动态治理。

**第十四条** 对于其他部门有共享需求，或师生应当知晓的数据，数据责任部门应当主动联络数据管理部门，将数据传输同步至数据平台，并完善展示页面供用户查阅，实现数据可视化。

**第十五条** 建立数据纠错机制，用户个人在展示页面对异常数据发起纠错，数据责任部门的数据管理员审核，审核结果反馈至展示页面并同步至业务系统，实现数据治理全联动、全流程、

可视化。

**第十六条** 建立数据共享机制，建立业务系统与数据平台同步机制。暂无能力提供数据接口技术支持的业务系统，数据责任部门暂时利用数据平台维护新数据,待业务系统升级迭代时解决。

**第十七条** 在新建或升级业务系统论证阶段，对系统数据建设情况进行评审论证，特别是数据标准遵循和数据收集范围；在验收阶段，承建方需提供数据库的结构设计、表结构、数据字典等相关技术文档。

## 第五章　个人信息保护

**第十八条** 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

**第十九条** 提高个人信息保护意识，充分尊重师生的知情权和决定权。在收集、处理个人信息时信息主体应知情并同意，存储传输个人信息应加密，公开信息应去标识化。

**第二十条** 处理个人信息应当采取对个人权益影响最小的方式，收集范围应当限于实现处理目的的最小范围，保存期限应当为实现处理目的所必要的最短时间。

**第二十一条** 生物识别、宗教信仰、特定身份、医疗健康、

金融账户、行踪轨迹等信息属于个人敏感信息，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下进行。

## 第六章　数据安全

**第二十二条** 按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，建立数据安全责任体系，将数据安全纳入网络安全责任体系，各单位（部门）负责人是第一责任人。

**第二十三条** 建立数据分类分级保护制度，加强对重要数据的保护。

**第二十四条** 加强数据增删改查等权限控制和日志管理，采取身份认证、访问控制等措施，防止未经授权的数据处理活动。采取措施保证数据安全，避免数据丢失或被破坏、更改和泄露。

**第二十五条** 系统建设单位需要与承建方签订数据安全保密协议。

**第二十六条** 不得超范围使用共享数据，不得以任何方式将数据用于社会有偿服务或其他商业活动。

**第二十七条** 开展数据安全宣传教育，组织管理和技术人员培训，加强宣传引导和教育，提升个人信息保护意识。提升数据安全防护水平，严格遵从数据安全和个人信息保护相关法律的明确防护要求,按照网络安全等级保护要求落实数据安全保障措施，提升防入侵、防泄漏、防滥用、防窃取能力。

**第二十八条** 对于违反法律法规规章和学校相关规定，造成国家、学校和个人损失的，学校将依法依规追究相关单位及个人的责任。

## 第七章　附　则

**第二十九条** 开展涉及国家秘密的数据处理活动，适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。在统计、档案工作中开展数据处理活动，开展涉及个人信息的数据处理活动，还应当遵守有关法律、行政法规的规定。其他未尽事宜，按照国家法律法规规章执行。

**第三十条** 本办法由网络安全和信息化委员会办公室负责解释。

**第三十一条** 本办法自 2022 年 12 月 1 日起施行。

大连海事大学网络信息与综合服务中心　　2022年12月1日印发