北京教育学院文件

京教院发〔2025〕1号

北京教育学院
关于印发《北京教育学院数据安全管理办法（试行）》的通知

各部门：

经学院2025年第1次院长办公会议审议通过，现将《北京教育学院数据安全管理办法（试行）》印发给你们，请遵照执行。

北京教育学院

2025年1月17日

北京教育学院数据安全管理办法（试行）

第一章　总　则

第一条 为进一步规范北京教育学院信息系统数据采集管理，推动数据归集整合，明确相关部门职责和权力，保障数据安全，实现学院信息系统数据的标准化管理，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》《中华人民共和国网络安全法》《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）、《信息安全技术个人信息安全规范》（GB/T35273-2020）和教育部等七部门《关于加强教育系统数据安全工作的通知》（教科信函〔2021〕20号）以及市教委相关文件要求，结合学院实际，制定本办法。

第二条 本办法所称的“数据”指各部门在履行职能时，通过信息化手段获取的业务数据和统计数据，覆盖数据全生命周期活动。

第三条 数据安全管理应遵循以下原则：

（一）数据统一管理原则。学院建设数据资源管理平台，负责学院信息系统数据的统一归集、共享、开放和使用。信息系统采集和处理的数据，应遵循学院制定的数据标准和接口标准。数据安全工作办公室应及时公开已经成熟明确的学院各级各类数据标准。各类信息系统在建设过程中，应主动做好与学院数据管理平台的数据对接工作。

（二）数据业务归口原则。应根据数据业务属性和职能部门的业务职能，将各类数据归属于相应部门，确定每一类数据的唯一权威，即遵循“一数一源”的原则。

（三）数据共享原则。学院建立统一数据共享通道和数据交换机制，除《中华人民共和国保守国家秘密法》所规定的涉密数据外，其他数据原则上允许院内各部门在其业务和管理范围内按需共享；数据共享需通过数据归属部门及数据安全工作办公室审核。

（四）数据安全管控原则。建立数据从采集、存储、传输、共享、使用、销毁的全过程管控体系。相关职能部门应定期检查、梳理业务范围内所负责的数据，确保数据质量。重点把好数据的采集关，确保源头数据真实、准确、完整、及时。

第四条 数据安全管理应达到以下目标：

（一）统一数据标准。学院逐步建立和完善统一的数据标准和管理规范，确保在信息系统建设过程中数据使用标准统一。

（二）保障数据完整准确。按照数据质量管理规范，实行数据质量核查机制，保障数据在各个环节的规范性、完整性和准确性。

（三）防止非法篡改和伪造。制定完善的数据所有权管理规范，明确数据的所有权及更改权限，确保对数据的所有权更改均有据可查，对于不可更改的数据，应提供相应的安全技术防止篡改和伪造。

（四）预防信息泄漏。根据国家和学院的安全保密工作要求，做好数据的保密工作，确保数据安全。

（五）提升数据服务质量。按照数据服务管理规范，全面提高数据质量、共享质量，充分发挥数据在学院发展中的重要战略作用。

第二章　组织结构和职责

第五条 学院成立数据安全工作领导小组（以下简称领导小组），组长由党委书记、院长担任，副组长由分管信息化院领导担任，成员由学院数据归属部门、数据使用部门、数据管理协调部门和数据技术管理部门负责人构成；领导小组负责学院数据安全工作的监督和管理，审定数据安全工作目标、工作计划、安全培训计划、安全策略方案、风险评估、追责机制并监督执行。

第六条 领导小组下设数据安全工作办公室，设在信息化办公室，主任由信息化办公室负责人兼任，负责领导小组日常组织和协调工作，制定数据安全工作目标、工作计划、安全培训计划、安全策略方案、风险评估、追责机制并落实执行，定期组织数据安全工作检查。

第七条 数据管理部门分为数据归属部门、数据使用部门、数据管理协调部门和数据技术管理部门。

第八条 数据归属部门是指根据工作职能采集会产生某类数据的部门，是该类数据的唯一权威来源，对该类数据有管理和审核权；并负责该类数据的采集、归集和质量管理，审核其它部门

对该类数据提出的共享申请。

第九条 数据使用部门是指因履行职责申请使用数据的部门。数据使用部门根据业务需要和数据使用的相关规定，提出数据使用申请，按规定在授权范围内合理、安全地使用数据。

第十条 数据管理协调部门及数据技术管理部门是指学院信息化管理和日常运维部门，负责学院信息系统数据共享与使用的协调、监督审核、技术支撑和保障。

第三章　人员管理

第十一条 学院数据归属部门、数据使用部门、数据管理协调部门和数据技术管理部门需设置专门岗位，依据职责分离的原则，明确其工作职责以及职能部门之间的协作关系和配合机制。

第十二条 学院加强对数据服务人员的管理，在录用重要岗位人员前需对其进行背景调查，并进行数据安全意识和专业能力测评，应符合相关的法律、法规、合同要求。

第十三条 数据服务重要岗位人员的兼职和轮岗、权限分离、多人共管等安全管理要求，需按最少够用原则为入职员工分配初始权限。在重要岗位人员调离或终止劳动合同前，相关部门与其签订保密协议，及时终止或变更离岗和转岗员工的数据操作权限，并及时将人员的变更通知到相关方。

第十四条 数据安全工作领导小组制定或修订数据安全培训计划，每年定期开展全员的数据安全教育和数据安全岗位人员专题培训，提升全员整体数据安全意识水平。

第五章　数据资产管理

第十五条 学院按照国家和教育行业有关标准要求，结合业务特点与需求等因素对数据进行分类，逐步建立和完善数据标准，通过数据资产管理工具形成支持即时更新的资产目录。

第十六条 资产目录需覆盖数据库、大数据存储组件、云上对象存储或网盘等存储工具、办公电脑、U 盘、光盘等存储媒体中的数据。

第十七条 采用技术手段定期对数据资产进行扫描，及时发现识别敏感信息。

第六章　数据生命周期管理

第十八条 数据采集

（一）定义。数据采集是指数据归属部门根据业务管理职能需要，通过信息系统或其他手段获取数据的行为。

（二）原则。采集部门应遵循“合法、必要、适度”和“谁主管、谁负责，谁提供、谁负责”的原则，按照“一数一源、一源多用”的要求，根据工作需要确定采集数据的范围，原则上不得重复采集。数据采集应遵循学院数据标准，做到真实、完整、规范、及时。

（三）管理要求。数据归属部门应在其职责范围内，制定和执行本部门业务管理领域的数据质量管理规范，做好数据的管理、更新和维护工作。当数据结构发生变更时，可根据业务需求和影响程度，按需向数据安全工作办公室提出数据标准修订申

请。

第十九条 数据归集

（一）定义。数据归集是指数据归属部门将依法履职过程中采集和产生的数据，根据数据管理要求，传输到学院数据资源管理平台。

（二）管理要求。

数据安全工作办公室制定相关的数据标准、工作流程，负责数据归集阶段的数据质量评价和监管，并从技术层面协助数据归属部门将本数据向学院资源管理平台归集。

数据归属部门根据工作职责确定归集数据的范围，按照统一标准编制、审核和发布本部门数据资源目录，作为学院数据共享、公开和业务协同的基础和依据，并及时提供、维护和更新归集数据，各方共同保证数据状态可感知、数据处理可明示、数据源头可追溯、安全责任可落实。

第二十条 数据共享

（一）定义。数据共享是指学院各部门间信息系统数据的共享，分为无条件共享、有条件共享、不予共享等三种类型。无条件共享，指在学院范围内，无需数据提供部门授权，经数据安全工作办公室审核后可供给各部门共享使用的数据资源；有条件共享，指在学院范围内，经数据提供部门授权，仅提供给部分部门共享使用的数据资源；不予共享，指不提供给其他部门共享使用的数据资源。凡列入不予共享类的数据资源，必须有国家法律、

法规等政策依据，除不予共享的数据外，有条件共享和无条件共享的数据必须通过学院数据资源管理平台实现交换共享。

（二）管理要求。

共享数据的提供部门应按照“谁主管、谁负责，谁提供、谁负责”的原则，及时提供、维护和更新共享数据，确保提供的共享数据与本部门数据一致。

申请阶段，数据使用部门应遵循“谁经手、谁负责，谁使用、谁负责，谁管理、谁负责”的原则，申请无条件共享数据时，应向数据安全工作办公室提出明确的共享需求和用途，经审核后通过学院数据资源管理平台获取共享数据。数据使用部门申请获取有条件共享数据时，应向数据提供部门提出明确的共享需求和用途，数据使用部门按答复意见使用共享数据；不予共享的，数据提供部门应说明理由。

授权阶段，凡通过审核的需求，由数据安全工作办公室组织数据提供部门、数据使用部门落实数据共享交换。数据使用部门遵循相关法律、法规以及共享审核结果所描述的用途，安全使用数据，并加强数据使用的全过程管理。

传输阶段，应尽量采用自动、实时的数据接口管道方式共享。采用数据复制或者其他调用方式的，征得数据归属部门和数据安全工作办公室的同意，过程中应进行加密确保数据安全。

数据安全工作办公室应建立数据流通监控平台和日志系统，实时展示、统计校内数据的共享流通情况，及时发现、解决数据

共享流通中出现的问题。

数据使用部门应当建立严格安全的数据访问控制机制，如有第三方数据分析需求，须经过审核后提供脱敏数据。对共享数据二次加工后得到的数据，其使用和安全由数据使用部门负责。

第二十一条 数据保管

（一）职责。数据安全工作办公室负责保管学院公共信息服务平台的数据，各部门负责保管本部门所属信息系统数据。

（二）要求。数据保管部门应当指定专人负责，建立数据备份制度，各部门负责本部门所属信息系统数据的定期备份或动态保存，及时完成数据备份，制定数据备份恢复方案，保证备份数据可恢复；此外，还须针对重大突发事件的特殊需求，制定数据存储和恢复的应急保障预案。

第二十二条 数据销毁

（一）定义。数据销毁是指通过一系列技术手段或物理方法，按照规定程序进行销毁，保证清除和销毁的彻底性，确保存储在各类介质中的信息数据达到无法被恢复或再次使用的目的。

（二）要求。

数据使用部门应须具有数据安全清理和销毁的意识，按照数据安全管理的要求清理和销毁本地临时数据、中间文件、过程文件。

数据管理技术部门可按照数据归属部门的要求清理和销毁原始数据。数据管理技术部门和数据归属部门销毁数据操作时须

记录清理和销毁数据过程，并接受安全管理人员审计。

第七章　数据合作方管理

第二十三条 凡参与学院信息化建设和服务的第三方，均须严格保障所涉及的数据安全。凡涉及重要数据信息的，须签订数据安全保障承诺书。如出现任何可能导致数据安全的违规操作，学院将保留追究其法律责任的权利。

第二十四条 应对数据合作方的数据安全能力进行评估或监督，确保合作方的保护能力与面临的数据安全风险相符。

第二十五条 应对合作方接入的系统、使用的技术工具进行技术检测，避免引入木马、后门等。

第二十六条 为完成技术或服务目的向合作方提供的数据，应在合作结束后进行回收，并要求合作方对数据进行删除。

第八章　数据安全管理要求

第二十七条 数据安全工作办公室组织开展安全风险评估、安全管理审查、安全质量考核及安全宣传教育培训，推进常态化数据安全监管机制。

第二十八条 加强数据的统筹授权使用和管理。鼓励在保护个人隐私和确保公共安全的前提下，按照“原始数据不出域、数据可用不可见”的要求，以数据模型、数据服务等形式向学院各部门提供，对不承载个人信息和不影响公共安全的公共数据，按用途加大供给使用范围，促进数据的共享使用，发挥数据效能。

第二十九条 各部门须定期对数据进行安全检查，加强业务

系统安全防护，建立应急处置、备份恢复机制，保障数据、平台安全、可靠运行，杜绝越权访问、错误授权等不当行为。数据生产部门和数据使用部门在数据共享交换工作中分别承担相应的安全保障责任。

第三十条 学院制定数据安全事件应急预案，建立数据安全应急处置流程，明确处置措施，开展数据安全监测预警与信息通报，定期开展数据安全事件应急演练，发现问题及时上报与处置。

第九章　数据安全投诉举报

第三十一条 数据安全工作办公室负责建立便捷的数据安全投诉举报渠道，按规定公布接受投诉、举报的联系方式、责任人信息，并及时受理、处置数据安全投诉举报。

第十章　附则

第三十二条 本办法由信息化办公室负责解释和修订。

第三十三条 本办法自发布之日起施行，其他文件规定与本文不一致的，按本办法执行。

北京教育学院党政办公室　　2025 年 1 月 17 日印发