

郑州工程技术学院文件

校政字〔2026〕51号

关于印发《郑州工程技术学院数据分类分级 实施细则》等两个文件的通知

学校各单位：

经学校校长办公会议研究通过，现将《郑州工程技术学院数据分类分级实施细则》《郑州工程技术学院“一数一源”数据资产管理办法》（试行）两个文件印发给你们，请结合单位工作实际，认真贯彻执行。

特此通知。



郑州工程技术学院数据分类分级实施细则

第一章 总 则

第一条 为规范数据资源的使用以及保障数据资源的安全，发挥数据资源在数据共享、大数据分析及辅助决策支持方面的作用，根据《中华人民共和国网络安全法》《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》《教育数据分类分级指南》（JY/T 0661—2025）等国家法律法规和行业标准，结合学校实际，制定本细则。

第二条 本细则适用于学校数据资源的分类分级工作。涉及国家秘密的数据分类分级按照相关保密法律法规的规定执行；涉及卫生健康、科技等行业领域的的数据分类分级，遵照相关行业领域标准规范执行。

第三条 学校数据分类分级工作实行“统一领导、分工负责、归口管理”的原则，由网络安全和信息化工作领导小组统一领导，信息与网络管理中心牵头组织，各业务部门负责本部门数据资产的梳理和初步分类分级工作。

第四条 本细则中的数据是指学校各类应用系统所涉及的相关数据，包括各类应用系统中的业务数据、系统数据、教学资源、档案资料及用户服务支持系统中的相关数据，以及经过统计、关联、挖掘、聚合等加工产生的衍生数据。涉及档案资料管理的，同时遵照《中华人民共和国档案法》及学校档案管理相关规定执行，本细则仅就数据安全分类分级事项进行规范。

第五条 本细则中的数据安全管理工作是指学校对数据全生命周期实施安全保护的管理活动，涵盖与数据相关的标准规范、规章制度、工作流程的制定完善，以及数据采集、录入、运维、存储、应用、共享、销毁等各环节的安全管理事项。

第六条 数据分类分级工作遵循以下基本原则：

（一）界限明确原则：各类别、各级别界限明确，每个数据集原则上只属于一个类别、一个级别。

（二）就高从严原则：当多个数据分级要素影响数据分级并出现不同级别时，以最高级别为准；当数据集包含多个级别的数据时，应按照数据的最高级别对数据集进行定级。

（三）动态更新原则：当数据业务属性、使用场景、公开范围等发生变化时，对数据分类分级目录进行动态更新。

第二章 管理目标

第七条 管理目标如下：

（一）确保数据完整准确。按照业务要求和数据质量管理规范，建立数据质量核查机制，保障数据真实、准确、完整和规范。

（二）确保数据安全可靠。按照数据安全管理工作规范，建立数据分级管理制度，落实数据存储与备份措施；明确数据的所有权和管理权限，做好数据操作的日志记录，保证数据更改的可追溯；根据国家、教育部和学校的相关要求，做好数据保密安全工作。

（三）提升数据服务质量。规范数据使用，建立数据共享管理机制。全面提高数据质量和提升管理服务水平，充分发挥数据在学校发展中的重要作用。

(四)符合行业监管要求。数据分类分级结果和保护措施符合国家和教育行业标准要求,重要数据和核心数据按规定报教育主管部门审批备案。

第三章 数据分类

第八条 按照《教育数据分类分级指南》要求,结合学校业务实际,学校数据分为以下6个一级类别:

(一)学生数据 指学校在开展学生管理和服务活动中收集和产生的数据集合,分为两个子类:

1.学生基础数据:学生及学生监护人的姓名、性别、民族、出生日期、籍贯、政治面貌、户口所在地、联系电话号码等个人信息,以及个人身份识别信息、个人健康生理信息、个人生物识别信息等敏感个人信息;对于不满十四周岁未成年人的个人信息,无论其类型,均应按敏感个人信息进行保护。

2.学生管理数据:招生录取数据、迎新数据、学生学籍数据、学生学历学位数据、学生实践活动数据、学生资助数据、学生毕业就业数据、学生心理健康数据、学生竞赛获奖数据、学生社团组织数据等。

(二)教职工数据 指学校在开展教职工管理和服务活动中收集和产生的数据集合,分为两个子类:

1.教职工基础数据:教职工及教职工家属的姓名、性别、民族、出生日期、籍贯、政治面貌、户口所在地、联系电话号码等个人信息,以及个人身份识别信息、个人健康生理信息、个人生物识别信息、个人财产信息等敏感个人信息。

2.教职工管理数据：教职工简历数据、教职工职务职称数据、教职工培养数据、教职工考核数据、教职工聘用数据、教职工薪酬福利数据、教职工离职数据、教职工普通话水平数据、干部人事数据、工会数据、纪检数据、离退休管理数据、港澳台教师管理数据、外籍教师管理数据等。

（三）教学管理数据 指学校在开展教学活动中收集和产生的数据集合，分为三个子类：

1.教务数据：教学计划数据、教学过程数据、选课数据、排课数据、考试成绩数据、实习实训数据等。

2.教学资源数据：课程教材数据、基本教学辅助资源数据、教室管理数据、数字教育资源数据、实验室运行管理数据等。

3.教学质量与评价数据：教学质量评估数据、教学评价数据、教学成果数据等。

（四）科研管理数据 指学校在开展科研管理活动过程中收集和产生的数据集合，包括科研项目管理数据、科研项目经费数据、科研项目考核数据、科研平台数据、科研成果及转化数据等。

注：本类别仅包含科研管理活动产生的数据，不包含科研原始数据，科研原始数据的分类分级遵照科技行业相关标准执行。

（五）校务管理数据 指学校日常运行过程中收集和产生的数据集合，分为九个子类：

1.党建德育数据：党组织管理数据、党员管理数据、党建活动数据、党内统计数据、德育活动数据、群团数据等。

2.学校概况数据：学校标识码、学校名称、学校地址、统一

社会信用代码、学校邮政编码、办学类型码、办学许可证号、校区基本信息、学校二级单位数据、学校历史沿革数据、学校学科门类数据等。

3.综合办公数据：公文数据、档案数据、会议数据、信息发布数据、学校组织架构数据等。

4.财务资产数据：预算数据、核算数据、决算数据、财会监督等财务管理数据、资产数据、审计数据、房地产与设施数据、仪器设备数据、软件资源数据、实验室数据、图书期刊数据等。

5.外事（港澳台）数据：来华留学数据、来内地（大陆）港澳台学生数据、出国留学数据、赴港澳台学习学生数据、来访数据、出访数据、港澳台专家数据、外籍专家数据、港澳台交流数据、国际交流数据等。

6.校友服务数据：校友基本信息、校友返校数据、校友捐赠数据等。

7.后勤管理数据：食堂管理数据、公寓管理数据、校园环境管理数据、校园修缮数据、物业数据、访客数据、安全保卫数据、安防交通数据、消防数据等。

8.安全数据：社会安全数据、事故灾害数据、考试安全数据、公共卫生与食品安全数据、网络安全数据、舆情监测数据、实验室安全数据等。

9.信息系统运行数据：用户数据、信息资产数据、配置数据、数字证书、日志数据、人工智能模型数据等。

（六）其他数据指不属于以上分类的其他数据。

第四章 数据分级

第九条 在数据分类基础上，根据数据重要性、敏感性以及数据一旦遭到泄露、篡改、破坏或者非法获取、非法使用、非法共享，对影响对象造成的影响程度，将学校数据级别分为重要数据（L4）和一般数据（L3、L2、L1）三级。

（一）L1 数据：是指国家、教育行业、学校公开的数据标准、代码信息，以及学校主动公开和依申请公开的行政数据和业务数据。一旦遭到泄露、篡改、破坏或者非法获取、非法使用、非法共享，可能对个人、学校权益造成一般危害。

（二）L2 数据：是指不予公开，但可在一定范围内共享的数据，包括各学院、部门和特定对象间共享的数据。按照职能收集并为公共服务、管理决策提供支撑的数据。一旦遭到泄露、篡改、破坏或者非法获取、非法使用、非法共享，可能对个人、学校权益造成严重危害。

（三）L3 数据：一旦遭到泄露、篡改、破坏或者非法获取、非法使用、非法共享，可能对经济运行、社会秩序、公共利益造成一般危害或者可能对个人、学校权益造成特别严重危害的数据。

（四）L4 数据：一旦遭到泄露、篡改、破坏或者非法获取、非法使用、非法共享，可能对国家安全造成一般危害或者对经济运行、社会秩序、公共利益造成严重危害。

第十条 数据分级动态调整

每年第一季度由信息与网络管理中心牵头，各业务部门配合

开展数据分类分级全面复核，更新数据分类分级目录。

当数据业务属性、使用场景、公开范围或数据规模发生重大变化时，数据产生部门应在 10 个工作日内提交重新定级申请，由信息与网络管理中心组织评审。

数据分级调整需进行完整日志记录，包括变更内容、变更原因、审批过程、生效时间等信息。

第五章 数据分类分级工作流程

第十一条 学校数据分类分级工作按照以下流程开展：

（一）数据资产梳理

各业务部门对本部门产生和管理的所有数据资产进行全面梳理，形成《部门数据资产清单》，明确每个数据集的责任部门、数据来源、覆盖范围、包含字段、更新频率、存储位置、访问权限等信息，形成完整的部门数据资产清单。

（二）数据分类分级初评

各业务部门按照本细则要求，对本部门数据集进行初步分类分级，填写《数据分类分级申报表》，提交至信息与网络管理中心。

（三）评审与报批

信息与网络管理中心组织网络安全、数据管理、法律等相关领域人员对各部门申报的分类分级结果进行评审，形成全校数据分类分级目录。其中：

L4 重要数据目录报教育部审批；

L1-L3 一般数据目录报上一级教育主管部门备案。

（四）结果发布与应用

经审批备案后的《学校数据分类分级目录》由信息与管理中心统一发布，各部门根据数据级别落实相应的安全保护措施，数据分类分级结果作为数据共享、开放、安全防护的重要依据。

（五）动态更新管理

数据分类分级目录每年定期更新一次，遇数据重大变更、业务场景调整或监管要求变化时随时更新，更新后需按原流程重新报批备案。

第六章 数据共享

第十二条 数据共享原则

（一）普遍共享

具有基础性、基准性、标识性的数据和数据提供方明确可以共享的数据可以普遍共享。

（二）有条件共享

数据内容敏感、按照学校保密管理或其他规定，经申请后在规定范围内提供给数据需求方（包括数据需求单位和个人）。

对于部分需要开放的数据，在不违反相关规定的条件下，需进行脱敏处理，对数据中涉及个人隐私或敏感内容的字段进行删除、替换或匿名化处理，使相关个人或机构无法被识别，并控制数据共享的类型与范围。

（三）不予共享

按照国家法律法规、学校规章制度或其他依据确定为不予公

开的数据，原则上不允许共享。

（四）申请最小使用范围原则

数据使用单位应当以满足实际业务需求为前提，按照最小范围原则申请共享基础数据资源。

第十三条 学校各学院、各部门在进行数据共享活动时，应约定共享数据的目的、范围、处理方式，采取必要的数据安全保护措施，并对数据共享活动进行监督。

第十四条 学校各学院、各部门负责所共享数据的安全管理，落实使用完毕的数据清理和销毁工作，销毁时采用不可恢复技术（如物理销毁或专业擦除工具）。

第十五条 学校各学院、各部门信息员应认真履行职责，发现数据下发异常的情况，应及时与信息与管理中心联系处理。

第十六条 注销的信息化项目或报废的存储设备，须按照本细则第十四条规定的不可恢复技术对承载的信息数据进行清理，确认清理完毕后，方可进行注销或报废处理。

第十七条 学校各学院、各部门若违反信息安全保密管理相关规定，造成敏感信息泄露，信息与管理中心需第一时间向网络安全和信息化工作领导小组报告，获领导小组批准后，有权关闭涉事方的数据接口权限，并责令责任部门限期整改。若涉嫌违法犯罪，案件移交司法机关处理的同时，需同步向学校相关领导报备。

第七章 数据安全事件应急预案

第十八条 数据泄露事件：系统由于受到外部攻击、内部人员违规操作或过失、系统漏洞等原因，造成数据被非授权访问、披露或流出的安全事件。当发现数据泄露时，应在2小时内上报网络安全和信息化工作领导小组，由网络安全和信息化工作领导小组办公室组织协调人员进行检查，采取技术措施及时阻止泄露扩散，评估泄露数据的范围和影响，并对受影响的个人或机构依法予以通知。L4及以上级别数据发生泄露事件时，需按要求同时上报上一级教育主管部门和网信、公安部门。

第十九条 数据篡改事件：系统由于受到外部攻击或内部人员违规操作，导致重要数据或核心数据对应的数据库及业务系统中的数据被非法修改的安全事件。当发现上述数据被篡改后，应在2小时内上报网络安全和信息化工作领导小组，由网络安全和信息化工作领导小组办公室指定运维人员进行检查确认，同时启动应急预案，暂停相关业务服务，通知相关业务部门，并保留原始日志及证据。L4及以上级别数据发生篡改事件时，须同步按第二十一条规定上报上一级教育主管部门和网信、公安部门。

第二十条 数据丢失事件：业务系统数据库、业务系统文件、办公文件数据等被非法删除、意外损毁或因存储介质故障导致数据无法恢复的安全事件。当发现数据丢失时，应在2小时内上报网络安全和信息化工作领导小组，由网络安全和信息化工作领导小组办公室统一指挥，组织协调相关部门进行检查，排查数据丢失影响范围，评估对业务的影响，并及时启动数据备份恢复程序，

尽快恢复业务正常运行。L4 及以上级别数据发生丢失事件时，须同步按第二十一条规定上报上一级教育主管部门和网信、公安部门。

第二十一条 当 L4 及以上级别数据发生安全事件时，由网络安全和信息化工作领导小组办公室按要求在 2 小时内上报上一级教育主管部门和网信、公安部门，配合相关部门进行协调处置。本条作为第十八条至第二十条外部上报要求的统一依据，各条款中涉及 L4 及以上级别数据安全事件的外部上报，均按本条规定执行。

第八章 附 则

第二十二条 本细则由网络安全和信息化工作领导小组负责解释。

第二十三条 本细则自发布之日起施行，原有规定与本细则不一致的，以本细则为准。本细则与国家或行业最新标准不一致的，以国家或行业最新标准为准。