丽水学院校长办公室文件

丽学院办〔2024〕52号

丽水学院校长办公室
关于印发数据安全和个人信息保护管理办法的通知

各部门、学院:

经2024年第9次校长办公会议审议通过，现将《丽水学院数据安全和个人信息保护管理办法》印发给你们，请遵照执行。

丽水学院校长办公室

2024年8月24日

丽水学院数据安全和个人信息保护管理办法

第一章 总则

第一条 为规范学校数据安全管理，加强个人信息保护，推动数据高效共享，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》等法律规定以及《教育部等七部门关于加强教育系统数据安全工作的通知》等精神，结合学校工作实际，制定本办法。

第二条 本办法所称的数据，是指校内各单位因教学、管理、服务等工作需要通过信息化手段采集、存储或使用处理的各类信息记录，不包括用于科学研究活动的各类原始数据及其衍生数据。涉密数据安全管理，按照相关标准和规定执行。非信息化手段采集的数据参考本规定执行。

第三条 信息化数据是学校公共资源，所有权和使用权归学校所有。数据安全管理工作坚持安全第一、分级保护、有效利用、合理共享的原则，严格遵守国家法律法规，落实数据安全主体责任，健全数据管理体制机制，推动提升校务治理能力，在做好信息保护的基础上充分发挥数据效能。

第二章 管理机制

第四条 网络安全工作领导小组是全校数据安全管理工作的领导和决策机构，负责贯彻落实上级重大决策部署和全校数据安全管理工作顶层设计与整体规划。

第五条 网络安全工作领导小组办公室（以下简称网安办）是全校数据安全管理的统筹协调部门，负责联系上级主管部门，制

定全校数据安全管理规章制度，协调做好数据安全管理领域重大突发事件应急处置工作。

第六条 按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，数据所属业务归口管理单位是数据主管单位，存储数据的网站和信息系统所属单位是数据运营单位，利用数据开展业务的单位是数据使用单位。按照“谁管业务、谁管业务数据、谁管数据安全”的原则，各单位党政主要负责人为数据安全第一责任人，相关分管领导为数据安全直接责任人。

第七条 数据主管单位负责制定归口管理的数据使用处理共享规则，明确防护要求，指导和督促各单位落实相关数据安全管理规定。数据运营单位负责制定网站和信息系统安全准则，落实数据主管单位防护要求。数据使用单位负责遵守数据使用处理共享规则以及网站和信息系统安全准则。

第八条 学校建立有效的安全管控流程，覆盖数据收集、数据存储、数据使用、数据加工、数据传输、数据提供、数据公开、数据删除全过程。

第九条 网安办是数据安全与信息保护工作的技术主管单位和关键数据平台运维单位，负责做好校级数据中台建设运行，制定数据安全管理技术标准，组织开展数据安全评估。

第十条 网安办牵头按照国家数据分类分级保护制度和上级单位有关规定，根据数据类型和重要程度，制定数据分类和分级原则，对数据实行分类分级管理。

第十一条 各单位根据职责，本部门所掌握的数据进行梳理，确定其共享属性，在公共数据平台进行目录编制，形成数据资产目录，并确保其准确性、完整性和合规性。

第十二条 各单位开展数据处理活动应采取技术和管理措施保障数据安全，按照“最小必要”的原则明确数据权限，实现数据管理、使用和安全审计权限分离，详细记录数据操作，相关日志保留时间不少于六个月。利用网络和信息系统开展数据处理活动，应按照有关要求，严格落实网络安全等级保护制度。

第十三条 学校建立数据开放共享制度，并建设数据中台支撑数据共享。数据使用单位或个人经所在单位审核同意，可对确定范围的数据提出使用申请，配合审批流程，加强共享数据使用全过程管理。网安办对共享需求和形式进行审核。鼓励通过在线接口和“用而不存”的方式使用共享数据。

第十四条 各单位针对内部信息系统制定安全运行管理流程，纳入网络与信息安全事件应急管理，组织开展演练，提高本单位信息安全应急响应能力。

第十五条 各单位规范细化安全应急事件处理流程，包括事件的发现、判断、评估、上报和处理等阶段，并落实本单位和应急处理管理机构的对口部门和人员，确保应急处理流程得到有效执行，信息安全事件得到有效控制和处理。各单位制定重要数据安全保障方案，并记录方案落实情况。

第十六条 各单位定期进行风险评估，了解网络信息系统目前可能存在的安全隐患和所面临的安全威胁，并针对本单位的实际情况，从物理、网络、系统、应用和数据等多个层面实施信息安

全保障工作。各单位定期对网络信息系统的运行状态、系统日志和安全日志等进行检查，对重要信息系统如网站、核心数据库等应每日进行运行检查，确保及时发现信息安全事件，减少安全事件所造成的损失。各单位定期或不定期组织预案演练，进一步明确应急响应各岗位责任，检验应急预案各环节之间的通信、协调、指挥等是否符合快速、高效的要求，对预案中存在的问题和不足及时补充、完善。

第十七条 网安办应举办安全教育培训，使不同岗位的人员都能熟悉并掌握相关信息系统的知识和技能。组织数据安全相关的技术和管理人员教育培训时间不少于 8 学时。

第三章 数据采集的安全保障

第十八条 未经网络安全工作领导小组批准，校内任何单位和个人不得以任何理由，私自收集学校范围内的师生、聘用人员等个人信息；各单位未经单位负责人批准，任何人不得以任何理由，私自收集本单位师生、聘用人员等个人信息。

第十九条 数据采集应遵循最小够用原则，明确采集依据、范围、场景和用途，原则上不得超越各单位的工作职能采集数据。

第二十条 新建信息系统应在建设方案中明确数据采集内容和数据等级。网安办应对数据采集的必要性和数据分级的合理性进行审核。

第二十一条 各单位对已建信息系统的数据采集项目建立数据资源目录，并全面归集到公共数据中心，如有新增数据采集的项目应及时更新报备信息。

第二十二条 各单位按照“一数一源”的原则，优先由学校数据共享平台匹配需求，原则上数据共享平台中已有数据应通过共享的方式获取数据。

第二十三条 各单位原则上不得自行采集学生、教师的个人生物识别信息。采集敏感数据或采集五百以上个人数据需报网安办审核批准。

第二十四条 各单位接收的数据，需跟数据提供方签订相关的协议明确双方的法律责任。

第四章 数据存储传输的安全保障

第二十五条 学校的内部数据和敏感数据应保存在学校数据中心，保存在校外（含云服务）的，需经网安办审核同意并严格落实数据安全责任。所有数据禁止保存在境外。

第二十六条 各单位使用的信息系统应根据数据安全级别采用数据加密、访问控制、数据防泄漏等安全措施。个人信息或敏感数据应采用符合国家要求的密码算法进行加密存储。实现存储数据的保密性、完整性和不可抵赖性。

第二十七条 各单位使用的信息系统应制定数据备份恢复策略和操作规范，对数据定期进行数据恢复演练，全量数据备份至少每周一次，增量数据备份至少每天一次，确保能够及时、完整、准确地恢复数据。

第二十八条 各单位应采用存储介质安全管控、校验技术、加密技术、数字签名等手段实现数据安全存储，不得直接提供存储系统的公共信息网络访问。应能够检测到数据在存储过程中保密

性、完整性、可用性受到破坏，在数据受到破坏时，应向授权用户提供告警信息。

第二十九条 在线的内部数据和敏感数据传输应采用加密传输，以保证数据传输的机密性和完整性；离线的内部数据和敏感数据加密后传输，且不得使用社会电子邮件系统、聊天平台等方式传递。

第三十条 应具备数据传输异常检测技术能力，对陌生 IP 地址、数据库异常连接等进行实时告警，在检测到数据遭破坏时及时采取恢复措施。

第三十一条 根据国家有关数据出入境相关规定，内部数据和敏感数据禁止出境；严格遵守“涉密信息不上网，上网信息不涉密”。

第五章 数据提供使用的安全保障

第三十二条 利用第三方平台开展数据活动的，应由数据运营单位和第三方平台提供者签订数据使用保密协议，明确数据提供的范围、数量、条件、程序等，落实数据安全责任。

第三十三条 信息系统使用单位应实现数据管理、数据使用和数据审计的权限分离；数据管理人员负责分配数据使用权限、按最小化原则授予各级各类人员的相关权限；数据使用人员根据业务和权限需要使用数据；数据审计人员负责对各类人员的数据操作进行审计记录和分析。

第三十四条 学校鼓励在保障数据安全的前提下，充分发掘数据潜在价值。对数据开展统计分析、科学研究、决策分析时，需经业务职能部门同意，且确保不泄露敏感信息，并对上述数据使

用行为进行记录。敏感数据使用前应采用适当的脱敏技术进行脱敏处理。

第三十五条 各单位通过加工产生的数据应与原始数据分开存储、保障原始数据的安全。

第三十六条 各单位应明确原始数据加工过程中的数据获取方式、访问接口、授权机制、逻辑安全、处理结果安全等内容，并周期性地检查用户操作数据的情况，统一管理数据使用权限。

第六章 数据共享公开的安全保障

第三十七条 根据数据分级确认数据共享策略。公开数据的共享和公开工作由网安办统筹负责，根据相关法规确定公开属性。内部数据的共享由网安办统筹负责，统一由网安办负责审核共享需求。敏感数据的共享由信息系统使用单位负责，自行决定是否共享。

第三十八条 内部数据和敏感数据不得用于商业用途。未经网安办同意，禁止与第三方共享。信息发布或共享使用前必须先经过脱敏处理，所有涉及人员身份、联系方式、学生学籍、人事、金融、资产、招生、科研、档案等中含有敏感信息数据的应采用屏蔽、变形、替换等多种手段来满足不同的隐私数据匿名化的数据合规性。

第三十九条 各单位在数据公开过程中需要有专职人员对数据公开过程进行校验，同时对可公开的内容进行二次审查。

第四十条 数据共享审核单位负责与被共享单位通过协议等方式确定数据共享范围、用途和安全责任，并将安全防护要求告知

被共享单位。被共享单位负责落实数据防护安全，保障数据不被窃取、滥用和篡改。

第四十一条 共享个人信息原则上通过接口方式实现，确需通过拷贝进行共享的，应报本单位领导同意，并由被共享方签订安全承诺书报网安办备案。

第七章 数据销毁托管的安全保障

第四十二条 对已过期确无保存价值的数据需销毁时，由数据管理人员提出数据销毁申请（并附销毁数据目录清单），经数据权属单位审核、主管领导审批核对确认后方可销毁。涉密数据销毁时，应依据保密法相关条例和数据保密等级实施销毁。数据销毁时，必须填写“数据销毁目录”，并有两人以上在场和签名。数据销毁后，数据管理人员应及时整理销毁过程有关资料归档。

第四十三条 各单位积极配合主管监管部门的数据安全检查工作、销毁重要数据及时向主管监管部门进行备案。

第四十四条 各单位通过签订合同协议等方式，明确委托方与被委托方的数据安全责任和义务。与委托方签订相关数据安全保密协议，同时对参与数据处理委托方相关人员进行信息留存备案。对被委托方的数据安全保护能力、资质进行评估或核实。

第八章 附则

第四十五条 本办法由网络安全领导小组办公室负责解释。

第四十六条 本办法自印发之日起施行。