郑州市教育局处室函件

郑教科信函〔2022〕564号

郑州市教育局办公室
关于加强全市教育系统数据安全工作的通知

各开发区教育局，各区县（市）教育局，局直属各学校（单位），市属事业及各民办学校：

为保障教育行政部门和学校利用信息化手段保护教学、管理、服务等环节产生数据的安全，规范数据收集、存储传输、使用处理、开放共享等数据活动，根据《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），现就加强全市教育系统数据安全工作的有关事项通知如下：

一、加强数据安全统筹协调

（一）加强数据安全组织领导。教育行政部门和学校应将数据安全纳入本单位网络安全管理体系，全面加强数据安全工作的组织领导，建立“主要负责人负总责、分管负责人具体抓”的领导责任制。加强对数据安全的顶层设计和统筹协调，明确网络安全职能部门应履行数据安全管理职责，建立健全数据全生命周期

的管理制度，为数据安全工作提供必要保障。

（二）健全数据安全责任体系。教育行政部门和学校应对本地区、本部门工作中产生、汇总、加工的教育数据及数据安全负主体责任，落实网络安全等级保护制度。按照“谁主管谁负责、谁运营谁负责、谁使用谁负责”的原则，数据所属业务的职能部门是数据的主管单位，应明确数据使用处理规则和防护要求；存储数据的信息系统（含网站，下同）主管单位是数据的运营单位，应制定信息系统安全准则，落实数据主管单位的防护要求；利用数据开展业务的单位是数据的使用单位，应遵守数据使用处理规则和信息系统安全准则要求。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和保密协议，明确使用方式、应用场景和使用边界，落实数据安全责任。

（三）建立数据分类分级制度。教育行政部门和学校应根据上级教育行政部门确定的教育系统重要数据保护目录，基础数据的防护要求，全面梳理本单位的数据，形成数据资源目录，准确掌握数据基本情况，做到底数清、情况明。按照数据在教育发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者非法获取、非法利用造成的危害性程度确定数据等级，对教育数据实行分类分级保护。

二 、规范数据生命周期管理

（一）规范数据收集工作。教育行政部门和学校应采取合法

正当的方式依法依规采集数据，并保障数据完整性、准确性和时效性。新建系统立项应对计划采集的数据进行分类分级，并对数据收集活动的合规性、合理性进行审核，已建信息系统新增、调整数据收集活动也应履行审核程序。按照“一数一源、最小必要”的原则，严格按照业务需要和职能边界确定数据收集使用范围，优先通过共享获取数据，不得重复收集数据。面向师生、家长收集信息应公开收集使用规则，明示收集使用目的、方式、范围和存储期限。

（二）规范数据存储传输工作。教育行政部门和学校应制定数据存储传输、备份恢复的安全策略。数据存储遵循“最短周期”原则，存储期限应当为实现处理目的所必要最短时间，超过期限的数据应进行归档或销毁。法律法规对存储期限另有规定的，从其规定。在境内运营收集和产生的非公开数据原则上应在境内存储。因业务需要，确需向境外提供的，应按国家有关规定开展数据出境安全评估。支持采用密码技术保障数据存储和传输的安全，密码技术和产品使用应符合国家密码管理部门要求。

（三）规范数据使用处理工作。教育行政部门和学校应按照“最小必要”的原则明确数据录入、查看、修改和删除等权限，实现数据管理、使用和安全审计的权限分离。应详细记录数据查询、录入、修改、删除和导出等操作，相关日志保留时间不少于六个月。采取身份认证、访问控制等技术措施，防止未经授权的

数据活动。鼓励在保障数据安全的前提下，充分发掘数据潜在价值。利用数据开展统计分析、科学研究、决策分析时，应经数据主管单位同意，并对数据进行必要的脱敏处理。

（四）规范数据开放共享工作。教育行政部门和学校应制定本单位的数据开放目录和数据共享责任清单，明确公开和共享的数据内容和范围。数据公开应遵从党和国家的有关要求，并建立完善的数据审核制度和重要信息的政策风险评估制度。建立数据共享的批准程序,数据主管单位明确数据的共享属性和防护要求;网络安全职能部门对共享需求和形式进行审核；数据使用单位遵守数据主管单位的防护要求，并接受数据主管单位和网信职能部门的监督。鼓励通过在线接口和“用而不存”的方式使用共享数据。

三、保障个人信息安全

（一）健全个人信息保护制度。教育行政部门和学校应提高个人信息保护意识，充分尊重师生、家长的知情权和决定权。收集处理个人信息应以显著方式、清晰易懂的语言展示收集处理规则，并经个人信息主体同意后方可实施。个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。不得以默认、捆绑、停止安装使用等手段变相强迫授权，不得违反法律法规和超越约定来收集处理个人信息。利用个人信息进行自动化决策，应当保证决策的透明度和处理结果的公平合

理。存储传输个人信息应采取加密措施，公开个人信息应采取去标识化处理。

（二）重点保护大规模个人信息。存储100万人以上个人信息的信息系统主管单位应明确个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。存储100万人以上个人信息的信息系统应向省级教育行政部门备案。收集和存储100万人以上个人信息的信息系统网络安全等级保护应定为三级以上，并每年对个人信息处理互动进行安全审计。教育行政部门和学校开发和使用的存储100万以上个人信息的教育App应通过个人信息安全认证，共享100万以上个人信息的应报省级教育行政部门审核同意方可实施。

（三）特殊保护儿童信息。教育行政部门和学校应对不满十四周岁的儿童信息实施特殊保障。收集处理儿童个人信息应当征得其监护人同意。严格控制儿童信息访问和管理权限，开展相关数据活动应征得数据主管单位同意，并采取技术措施记录访问情况。共享儿童信息应严格按照数据共享责任清单的范围，原则上不得向第三方共享儿童信息，确需共享时应进行数据安全评估并签订安全责任书。除法律法规要求和监护人约定，不得披露儿童信息。未经儿童监护人及本人同意，不得将儿童的数字画像用于商业用途。

（四）严格保护敏感个人信息。种族、民族、宗教信仰、个

人生物特征、医疗健康、金融账号、个人行踪等信息属于敏感个人信息。收集处理敏感个人信息应对必要性、科学性、伦理性进行论证，并经单位领导班子集体决策同意后方可实施。实施时应取得个人信息主体的单独同意，并告知使用敏感个人信息的必要性以及对个人的影响。在公共场所采集图像采集、个人身份识别信息的，应为维护公共安全所必需，只能用于维护公共安全的目的，不得公开或向其他提供。鼓励基于人口库等权威数据源，以“用而不存”的方式处理敏感个人信息。

四 、健全数据安全保障体系

（一）加强数据安全制度建设。教育行政部门和学校应制定本单位的数据安全管理办法，规范数据分类分级，明确数据安全防护措施。将数据泄露、破坏等数据安全事件纳入本单位网络安全事件应急预案中，明确处置措施。发生数据安全事件应按规定及时告知用户并向相关教育行政部门报告。

（二）开展数据安全宣传教育。教育行政部门和学校应定期组织管理和技术人员培训，特别是数据活动相关的关键岗位的培训，切实提高数据安全意识和防护能力。加强宣传引导和教育，以开学教育、网络安全宣传周等活动为契机，培养师生科学的网络使用习惯，重点提高防范电信网络诈骗和信息泄露的意识。通过专题培训、专题报告等形式，促进家长树立正确的用网观念，切实履行监护人的权力，全方位地提高广大师生、家长的信息素

养和个人信息保护意识。

（三）提升数据安全防护水平。教育行政部门和学校应严格遵从数据安全和个人信息保护相关法律法规明确的防护要求，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。加强对数据安全工作的经费支持，保障数据分级分类、安全评估、安全防护等重点任务开展。支持优先使用自主可控的软硬件设备和密码技术，保障教育系统数据安全。鼓励利用大数据、区块链、人工智能、可信计算等新技术、新应用，提升数据安全保障水平。

2022 年 8 月 23 日