北京市第一〇一中学教育教学数据安全管理规定

第一章 总则

第一条 制定目的

为规范北京市第一〇一中学（以下简称“学校”）教育教学数据的处理活动，加强数据全生命周期安全管理，保障数据安全与合理利用，促进数据驱动的教育教学创新，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》《北京市第一〇一中学数据安全与个人信息保护管理办法》等相关法律法规及学校制度，结合教育教学工作实际，制定本规定。

第二条 适用范围

本规定适用于学校在教育教学活动过程中产生、采集、存储、使用、共享、公开和销毁的各类数据的安全管理活动。包括但不限于：

1. **学生学习过程数据：**课堂互动记录、在线学习行为日志、作业完成数据、测验与考试成绩、综合素质评价记录等。
2. **教师教学行为数据：**教学设计、课件、课堂实录（音视频）、教学反思、教研活动记录、学生学业评价数据等。
3. **课程与资源数据：**数字教材、校本课程资源、微课、题库、虚拟仿真实验等数字化教学内容。
4. **教学管理数据：**排课信息、选课记录、考务安排、教学质量监测与分析报告等。
5. **教育评价与发展数据：**学生成长档案、教师专业发展档案、学校教学质量评估报告等。

第三条 管理原则

教育教学数据安全管理遵循以下原则：

1. **教育导向原则：**数据安全管理应服务于立德树人根本任务，促进教育教学质量提升和学生全面发展。
2. **分类分级原则：**根据数据的重要程度、敏感程度及遭到篡改、破坏、泄露或非法利用后可能造成的危害，对教育教学数据实行分类分级保护。
3. **最小必要原则：**数据收集范围应限于实现教育教学目的所必需的最小范围，禁止过度收集。
4. **安全可控原则：**在保障数据安全的前提下，促进数据在授权范围内的有序共享和合理利用。
5. **责任明确原则：**明确数据产生、管理、使用等各环节的安全责任主体。

第二章 组织与职责

第四条 领导机构

学校网络安全与信息化工作领导小组负责统筹指导全校教育教学数据安全管理工作，审议相关重要政策和重大事项。

第五条 归口管理部门

教导处是教育教学数据安全管理的归口责任部门，主要职责包括：

1. 制定并组织实施教育教学数据安全管理相关细则和流程。
2. 指导各学科组、年级组规范开展教育教学数据处理活动。
3. 审批重要的数据收集、使用、共享申请。

4. 组织开展面向教师的教育教学数据安全与合规使用培训。

5. 会同信息技术中心开展数据安全风险评估与检查。

第六条 技术支持部门

信息技术中心负责为教育教学数据安全管理提供技术支撑，包括：

1. 建设并维护安全可靠的数据存储、处理和分析环境。

2. 实施数据加密、访问控制、安全审计等技术防护措施。

3. 定期对承载教育教学数据的系统进行安全检测与漏洞修复。

4. 提供数据备份与恢复技术支持。

5. 监测数据安全态势，协助处置数据安全事件。

第七条 数据责任人员

1. **数据产生者：**教师、学生在教学活动中生成数据时，应遵循相关规范，确保初始数据的准确性与合规性。
2. **数据处理者：**各学科组、年级组、职能部门在职责范围内处理数据时，须严格遵守本规定，确保数据处理活动安全合法。
3. **系统管理员：**负责相关教育技术系统的管理人员，须落实系统层面的数据安全配置与管理要求。

第三章 数据全生命周期安全管理

第八条 数据采集

1. 采集教育教学数据必须有明确、合法的教育教学目的，并在采集前以适当方式（如家长告知书、平台隐私政策）向学生及监护人明示采集的目的、方式、范围、存储期限及权利保障途径，依法获取同意。

2. 严禁采集与教育教学无关的学生生物识别信息、家庭财务状况、家长职务等信息。确因特殊教育需要采集学生健康等敏感信息的，须经严格审批并采取强化保护措施。
3. 鼓励采用去标识化、匿名化技术手段在采集环节降低数据敏感性。

第九条 数据存储与传输

1. 教育教学数据应存储在由学校信息技术中心统一管理和维护的服务器或经安全评估的可靠云服务平台。原则上不得存储在教师个人电脑、私人网盘或未经认可的第三方平台。
2. 根据数据分级（参考学校数据分类分级规范）采取差异化的存储保护措施。核心教学评价数据、学生敏感个人信息等应加密存储。
3. 在校内网络传输一般教育教学数据需保障通道安全。通过互联网传输敏感数据或批量数据时，必须使用加密传输方式（如 VPN、SSL/TLS）。

第十条 数据使用与加工

1. 数据的使用应严格限定于采集时声明的目的范围内。因教研、质量分析等需要超出原范围使用的，应进行安全影响评估并重新获得授权。
2. 教师在教学分析和个性化指导中使用学生数据时，应遵循专业伦理，保护学生隐私和自尊，禁止公开排名、对比等可能伤害学生的数据使用方式。

3. 对数据进行统计、分析、挖掘等加工活动时，如可能产生新的衍生数据或识别出个体，应评估其敏感性并采取相应保护措施。对外发布的研究报告应使用聚合的、去标识化的数据。

第十一条 数据共享与提供

1. 原则上不向学校以外的组织或个人提供原始教育教学数据。确因教育研究、区域质量监测等需要提供的，须经教导处审批，并签订数据安全协议，明确数据用途、保护责任和销毁要求。
2. 在校内各部门间共享数据，应遵循“按需共享、权限最小化”原则，履行内部审批手续。
3. 向学生本人或其监护人提供个人数据查询、下载等服务时，应通过安全可信的身份验证机制。

第十二条 数据公开与发布

1. 公开涉及学生个体的成绩、评价、作品、图像、视频等数据，必须事先征得学生本人及其监护人的明确书面同意。公开涉及教师个人的教研成果、教学实录等，须征得教师本人同意。
2. 在学校官网、公众号等平台发布教育教学相关统计数据、成功案例、活动报道时，应进行必要的脱敏处理，避免泄露师生可识别信息。

第十三条 数据留存与销毁

1. 教育教学数据的留存期限应遵循国家档案管理规定及教育教学实际需要。学籍数据、重要学业成绩等应长期保存。
2. 超出留存期限或处理目的已实现的数据，应定期进行安全销毁。

存储在电子设备上的数据应采用不可恢复的方式彻底删除；纸质数据应作碎化处理。

3. 学生毕业或教师离职后，其相关数据的处理应遵循学校档案管理规定及个人信息保护要求。

第四章 重点场景与系统安全管理

第十四条 智慧课堂与录播系统

1. 课堂实录（含音视频）属于敏感数据，录制前应明确告知师生录制目的、保存期限和使用范围。未经同意，不得随意录制、传播。
2. 录播数据应存储在指定安全区域，严格设定访问权限。回放、教研使用需经授权。

第十五条 在线学习平台与教育 APP

1. 选用的在线学习平台或教育 APP 必须具备合法的备案资质，其数据收集、使用政策应符合国家规定和学校要求。
2. 平台应能提供符合学校要求的数据导出、删除接口，保障学校的数权和对学生数据的管控能力。
3. 教师应引导学生规范使用，注意保护个人账户安全和隐私信息。

第十六条 学业评价与成绩管理系统

1. 成绩数据是核心敏感数据，其录入、修改、查询、统计等操作必须留有完整、不可篡改的审计日志。
2. 严禁任何人员未经授权泄露、传播学生成绩及排名信息。成绩通知应直接送达学生本人或监护人。

第十七条 教育大数据分析应用

1. 开展基于教育教学数据的分析、预测等应用，应进行伦理和安全审查，防止算法歧视或不当标签化。
2. 分析结果的使用应服务于改进教学、促进学生发展，避免用于对师生进行简单量化考核或施加不当压力。

第五章 安全事件应急与责任追究

第十八条 应急响应

发生教育教学数据泄露、篡改、丢失、滥用等安全事件时，涉事人员须立即报告教导处和信息技术中心，并启动应急预案。学校须依法依规及时处置，并向受影响个体和上级主管部门报告。

第十九条 监督检查

教导处和信息技术中心应定期（每学期至少一次）对教育教学数据安全管理情况进行联合检查或审计，发现问题督促整改。

第二十条 培训宣传

学校应定期组织全体教师进行数据安全与隐私保护培训，提升教师的数据素养和合规意识。通过家长会、宣传栏等渠道向学生及家长普及数据安全知识。

第二十一条 责任追究

对于违反本规定，造成教育教学数据安全隐患或事件的部门和个人，学校将依据相关规定视情节轻重给予批评教育、通报批评、行政处分等处理；构成犯罪的，依法移送司法机关。

第六章 附则

第二十二条 本规定由学校网络安全与信息化工作领导小组负责解释。

第二十三条 本规定未尽事宜，按照国家有关法律法规及学校相关制度执行。

第二十四条 本规定自发布之日起施行。