北京市第一〇一中学师生个人信息保护专项规定

第一章 总则

第一条 制定目的

为切实保护北京市第一〇一中学（以下简称“学校”）师生个人信息安全，规范个人信息处理活动，维护师生合法权益，促进学校教育教学活动安全有序开展，根据《中华人民共和国个人信息保护法》《中华人民共和国未成年人保护法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》及相关法律法规、上级主管部门要求，结合本校实际，制定本规定。

第二条 适用范围

本规定适用于学校及全体教职工（包括在编、外聘、劳务派遣等各类人员）、在校学生（含幼儿）个人信息的处理活动。

学校委托第三方处理个人信息，或向第三方提供师生个人信息的，适用本规定及学校相关合同管理制度。

第三条 基本定义

1. **个人信息：**指以电子或者其他方式记录的与已识别或者可识别的师生有关的各种信息，不包括匿名化处理后的信息。
2. **敏感个人信息：**指一旦泄露或者非法使用，容易导致师生的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。学生学籍信息、家庭情况、成绩、体检报告、教职工人事档案、薪

资信息等均属学校管理中的敏感个人信息范畴。

3. **个人信息处理：**包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。

第四条 基本原则

处理师生个人信息，应严格遵循合法、正当、必要和诚信原则，并符合以下要求：

1. **目的明确与最小必要：**具有明确、合理的目的，且与学校履行法定职责、提供教育服务直接相关。仅限处理实现目的所必需的最少信息。
2. **公开透明与知情同意：**公开个人信息处理规则，明示处理的目的、方式和范围。除法律、行政法规另有规定外，处理个人信息应当取得个人的单独同意或符合法定情形；处理不满十四周岁未成年人个人信息，应当取得其监护人的同意。
3. **安全保障与责任落实：**采取必要措施保障所处理个人信息的安全，防止未经授权的访问、泄露、篡改、丢失，并指定专门部门及负责人落实保护责任。

第二章 组织与职责

第五条 领导机构

学校网络安全与信息化工作领导小组（或专项设立的个人信息保护工作领导小组）全面领导学校师生个人信息保护工作，负责审议相关重大政策，协调解决重大问题。

第六条 责任部门

教导处为学生个人信息保护工作的主要责任部门，校办公室为教职工个人信息保护工作的主要责任部门，共同履行以下职责：

1. 制定并落实本部门相关个人信息处理活动的管理细则和操作规程。
2. 组织开展对本部门教职工的个人信息保护宣传与培训。
3. 受理、初步核实与本部门相关的个人信息保护咨询与投诉。
4. 配合信息技术中心等部门开展安全检查与风险评估。

第七条 技术支持与监督部门

信息技术中心是个人信息保护的技术支持与监督部门，主要职责包括：

1. 为个人信息处理活动提供安全可靠的技术环境，实施必要的技术防护措施。
2. 定期对信息系统中的个人信息处理活动进行安全监测、风险评估和合规性检查。
3. 在发生或可能发生个人信息泄露、篡改、丢失时，牵头采取技术措施进行遏制和补救。
4. 指导各部门规范处理个人信息。

第八条 个人信息保护负责人

学校指定一名校级领导担任个人信息保护负责人，负责统筹协调全校个人信息保护工作和相关事务，其姓名及联系方式依法向社会公开。

第三章 个人信息处理全流程规范

第九条 收集环节

1. **源头控制：**严格执行“非必要不收集”原则。任何新增的师生

个人信息收集需求，均需由业务部门提出申请，明确法律依据、收集目的、信息范围、使用方式、存储期限，经责任部门及个人信息保护负责人审批同意后方可实施。

2. **告知同意：**收集前，须通过清晰易懂的语言（特别是面向学生和家长时）以书面、公告、电子协议等形式，真实、准确、完整地告知本规定第四条第二款所列事项，并依法取得同意。禁止以欺骗、误导、胁迫等方式收集。
3. **重点保护：**收集不满十四周岁未成年人个人信息，必须取得其监护人的明确同意，并验证监护人身份。

第十条 存储与使用环节

1. **分类分级存储：**根据《北京市第一〇一中学数据分类分级管理规范》，对个人信息进行标识和管理。敏感个人信息应当加密存储，并在技术上实现与一般个人信息相隔离的访问控制。
2. **访问权限控制：**严格遵循“最小权限”原则，根据岗位职责为教职工分配访问权限。访问师生敏感个人信息，须经过二次授权或审批。建立并定期复核访问权限清单。
3. **使用限制：**个人信息仅限用于收集时告知并经同意的目的。因教育教学、管理、安全等确需超出原范围使用的，应当重新履行告知同意程序。禁止以任何形式非法买卖、提供或者公开师生个人信息。

第十一条 加工、传输与提供环节

1. **加工安全：**因统计、研究等目的需要进行个人信息加工（如去

标识化、匿名化）时，应采取技术和管理措施，确保加工后的信息无法重新识别特定个人，且加工过程安全可控。

2. **传输安全：**通过互联网或公共网络传输敏感个人信息，必须使用加密通道（如 VPN、HTTPS）等安全措施。
3. **对外提供：**原则上不得向学校以外的任何组织或个人提供师生个人信息。确需向教育主管部门、合作医疗机构等提供的，应当进行安全影响评估，签订含有严格保密条款和数据安全保护责任的协议，并记录提供情况。

第十二条 公开与删除环节

1. **审慎公开：**原则上不公开师生个人信息。确因表彰、宣传等需要在官网、公告栏等公开学生姓名、照片等信息的，须事先征得学生本人及其监护人的明确同意；涉及教职工的，须征得本人同意。
2. **及时删除：**在达到存储期限（根据法律规定、合同约定或处理目的确定）或处理目的已实现后，应当主动或依师生请求删除个人信息。法律法规要求留存的信息除外。删除应采取不可恢复的技术手段。

第四章 特别保护规定

第十三条 未成年人个人信息特别保护

处理学生个人信息，尤其是未成年学生信息，除遵守一般规定外，还应：

1. 制定专门的未成年人个人信息处理规则。

2. 处理前进行个人信息保护影响评估，并对处理情况进行记录。
3. 加强对教职工的培训，使其充分认识未成年人个人信息保护的特殊重要性。
4. 定期以学生及家长易于理解的方式，说明个人信息处理情况和保护措施。

第十四条 人脸、指纹等生物识别信息管理

1. 除为维护公共安全且依照国家有关规定在特定场所使用外，原则上不在校园门禁、考勤、支付等场景中收集使用师生的人脸、指纹等生物识别信息。
2. 确需使用的，必须进行严格的必要性、安全性论证和风险评估，制定专项安全管理规定，获得个人信息保护负责人批准，并取得师生或其监护人的单独书面同意。
3. 生物识别信息应与身份信息分开存储，原则上不得存储原始生物识别信息（如图片、模板），应采用不可逆技术处理后存储。

第五章 安全事件应急与权益保障

第十五条 应急响应

发生或可能发生个人信息泄露、篡改、丢失等安全事件时，应立即启动《北京市第一〇一中学网络安全事件应急预案》中数据安全事件专项流程。信息技术中心须立即采取补救措施，责任部门和个人信息保护负责人须按规定及时上报，并依法告知受影响的个人（及其监护人）。

第十六条 投诉与举报

学校建立师生个人信息权益保障渠道。师生或其监护人认为个人信息

处理活动违反法律、行政法规或本规定，侵犯其合法权益的，有权向学校责任部门或个人信息保护负责人投诉、举报。学校应在 15 个工作日内进行调查、处理和反馈。

第十七条 权利行使

师生及其监护人依法享有对本人个人信息的知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理（法律、行政法规另有规定的除外），有权查阅、复制、更正、补充、删除其个人信息。学校应建立便捷的申请受理和处理机制。

第六章 监督、考核与责任追究

第十八条 监督检查

信息技术中心会同责任部门，每学期至少组织一次个人信息保护专项检查或合规审计，检查结果报学校网络安全与信息化工作领导小组。

第十九条 培训与考核

学校将个人信息保护知识纳入全体教职工常规培训内容，新入职教职工必须接受相关培训。个人信息保护责任制落实情况纳入相关部门及人员的年度绩效考核。

第二十条 责任追究

对违反本规定，有下列行为之一的部门或个人，学校将视情节轻重，给予批评教育、通报批评、取消评优资格、行政处分等处理；造成损害的，依法承担民事责任；构成犯罪的，依法移交司法机关追究刑事责任：

1. 未履行个人信息保护义务，导致发生安全事件的。

2. 未经授权或超出授权范围访问、使用、提供、公开个人信息的。

3. 非法买卖师生个人信息的。

4. 其他违反法律法规和本规定的行为。

第七章 附则

第二十一条 本规定由学校网络安全与信息化工作领导小组负责解释。

第二十二条 本规定自发布之日起施行。学校原有规定与本规定不一致的，以本规定为准。