杭州师范大学文件

杭师大发〔2023〕7号

杭州师范大学关于印发信息系统数据管理办法（修订）的通知

各学院（部）、部门：

现将《杭州师范大学信息系统数据管理办法（修订）》印发给你们，请认真遵照执行。

杭州师范大学

2023年5月31日

杭州师范大学信息系统数据管理办法
（修订）

第一章　总则

第一条　为进一步加强学校信息化建设统筹规划，建立有效的信息系统数据共建、共享与保障体系，提高数据质量和利用效率，为学校推进数字化改革提供安全可靠、完整统一的数据信息，根据相关法律、法规及规范要求，结合学校实际，修订本办法。

第二条　本办法所指的信息系统数据是指学校各类信息化业务系统（以下简称信息系统）建设、使用过程中产生或获取的各类数据，但不包含《中华人民共和国保守国家秘密法》及其他各项法规规定的涉密数据。

第三条　信息系统数据管理是指学校各部门利用信息系统或相关数据管理平台对教学、科研、管理和服务等业务数据进行收集、归集、存储、加工、传输、共享、开放、利用、保护等数据管理的工作。

第四条　管理原则

（一）统一标准原则。信息系统数据管理应符合国家、教育部、行业、学校等制定的相关标准与规范。

（二）归口管理原则。各类数据在纳入统一平台管理的基

础上，按业务属性由学校各业务管理部门进行归口管理。

（三）安全共享原则。在保证数据安全的前提下，实现数据共享以及衍生数据应用服务，使数据能够满足各种业务使用需要。

（四）全程管控原则。建立数据从采集、维护、存储、归档、应用、保护的全过程管控平台和制度体系，确保数据真实、准确、完整、及时。

第五条 管理目标

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

（二）确保数据安全可靠。按照数据安全管理规范，建立数据分级管理与备份、容灾和恢复机制；明确数据的所有权和管理权限，做好数据操作日志记录，保证数据更改可追溯；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。

第二章 职责分工

第六条 学校网络安全和信息化工作领导小组是学校信息系统数据管理的领导机构，负责政策制定、顶层设计和学校数据管理等重大事项决策。

第七条 信息中心在领导小组领导下，负责协调和推动学校信息系统数据管理具体工作，负责全校信息系统数据管理总体规划和技术平台支撑等工作，主要包括：

1.制定信息系统数据资源的总体规划，制定和执行学校信息编码标准、技术规范、管理规程等；

2.信息系统数据中心平台软硬件建设，做好数据中心安全运维工作；

3.协助各部门做好各类数据维护和使用，统筹协调推进信息系统数据共享等工作。

第八条 按照“谁生产、谁治理、谁负责”原则，各部门根据部门职责和业务分工，是相应数据的生产部门和权威单一来源部门，负责本部门数据规划、生产、治理等各项数据管理工作，对数据质量负责，并按要求向学校数据中心提供权威数据。

第三章 数据分类分级

第九条 数据分类：根据学校业务分类，信息系统数据分类与归口管理如下：

（一）教师类。教职工基本信息、人员招聘、入职离校、职务评聘、考核管理、培训管理、人才管理、奖惩管理、薪资管理、党团工作、出国证件管理、出国（境）出访以及离退休等相关数据。

（二）学生类。本科生、研究生、函授生、国际学生等所

有与学生相关的基本信息，以及迎新、奖惩、奖学金、党团、毕业、就业、校友和生活等相关数据。

（三）教学类。本科生、研究生、国际学生等所有与学生相关的招生、学籍、教学计划、排课、选课、成绩、学位等；学生评教、教学改革、专业、课程、教学资源等相关数据。

（四）科研类。科研项目管理、合同管理、各类成果管理、科研机构管理、科研平台、科研团队、科研经费管理、科研业绩考核等相关数据。

（五）社会服务类。教育合作、教育培训、其他产学研合作、校企（政）科研机构管理、科技成果转化等相关数据。

（六）财务类。财务管理、经费管理、教职工薪资发放、学生收费信息等。

（七）资产类。采购管理、固定资产管理（含图书文献资料）、实验室管理、设备管理、房产管理、土地管理等相关数据。

（八）数字档案类。人事档案管理、学生档案管理、文件档案管理、科研档案管理等相关数据。

（九）公共类。校园一卡通、校园网络服务、门禁信息、网站信息、电子邮件、水电气能耗、车辆信息等。

（十）系统数据类。包括网络出口数据、访问数据、数据库连接数据、应用系统安全数据等实现网络连接、操作系统管理、数据库管理、应用系统功能等相关数据。

（十一）其他数据。学校日常管理产生的其他相关数据。

第十条 数据分级：基于数据重要性、敏感性、影响对象及程度确定数据等级，根据数据等级明确保护措施。

（一）第一级数据。即公开数据，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。

（二）第二级数据。即内部数据，是指不予公开，但可在一定范围内共享的数据，包括各部门、学院、附属医院和特定对象间共享的数据。按照职能收集并为教学、科研、管理决策等提供支撑的数据。

（三）第三级数据。即敏感数据，是指涉及学校秘密的相关数据，一旦遭篡改、泄露、丢失、损毁后，对学校安全或利益造成损害的数据。

（四）第四级数据。即高敏数据，是指一旦遭篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成严重损害的数据。

业务部门须根据分级要求确定数据等级，并报信息中心备案。确定为第三、四级数据的，经信息中心审核后，报网络安全和信息化工作领导小组审定。

第四章 数据维护

第十一条 数据维护是指学校各部门利用相应的信息系统等数据管理平台（如各部门建设管理的信息系统、学校数据中

心提供的数据接口、学校数据中心提供的数据管理平台等），根据数据归口管理权限，遵照本部门业务规范及学校信息编码标准，进行统一的数据采集录入、补充更新等操作。

第十二条 各部门应根据部门实际，分类制定和实施信息系统数据维护的技术性方案和操作办法。

（一）已建立信息系统的部门。提供相应信息系统的设计文档、数据字典和数据接口等资料，通过系统集成，将各类业务数据维护至学校数据中心平台。相关信息系统在变更其数据结构等操作时，须提前向信息中心报备，避免数据混乱及服务异常。

（二）未建立业务系统的部门。数据归口管理部门应根据实际需要提出需求，联合信息中心制定数据采集和集成标准，依托学校数据中心平台，通过技术开发制定数据导入接口，相关部门利用接口做好数据导入维护，逐步实现相关数据集成。

第十三条 各部门进行数据维护时，应保证数据的真实性、完整性、规范性和时效性。

（一）真实性。各部门应准确维护相关数据，不得随意修改、增减。

（二）完整性。各部门须确保数据完整、齐全，避免数据缺失。

（三）规范性。各部门遵循“一数一源”的原则，学校数据中心平台可以获取的数据，原则上不得重复采集，确保数据

规范可用。

（四）时效性。各部门须在规定的时间内进行数据维护，确保数据与实际业务同步，防止产生无效数据、过时数据。

第十四条 各部门应明确数据维护责任人、权限和具体职责，制定和执行数据质量管理规范，规范数据维护操作程序。数据维护相关人员，应严格按照规程及时维护数据，定期更改系统认证口令，严禁在未按规定授权的情况下委托他人进行数据维护，确保学校数据安全。因系统故障、误操作、信息泄露等原因导致数据维护重大问题的，应及时向信息中心报告，以便及时处理。

第五章 数据存储

第十五条 信息中心利用学校数据中心平台，负责全校各类信息系统数据的采集、清洗、整合、归档、存储、备份、恢复、共享等工作。

第十六条 暂未纳入学校公共数据中心统一存储的信息系统数据，由归口管理部门负责数据本地备份和归档等各项数据维护工作。

第十七条 档案馆应根据上级有关规定和行业规范，建立独立于学校数据中心电子档案数据管理平台，独立开展电子档案数据维护、存储、归档、使用、保护等工作。

第六章 数据共享使用

第十八条 信息中心负责建立和运营统一的数据中心管理

平台，协助相关部门开展信息系统数据日常使用与管理工作。

1.建立学校公共数据中心数据存储、数据交换、数据共享平台，提高业务系统的数据集成、共享与应用水平；

2.逐步建立数据决策支持平台，为学校提高管理效率和科学决策，提供数据信息服务；

3.逐步建立分布式信息服务平台，建立面向师生个人服务的个人数据中心，全面展示师生个人在校内的工作、学习和生活等方面的数据和信息，在此基础上逐步提供各类网上办事审批业务等简化师生填表服务。

第十九条 校内各部门因工作需要须通过学校数据中心获取跨部门信息系统数据的，应根据“按需够用”原则，填报《杭州师范大学信息系统数据使用审批单》（附件1）、《杭州师范大学数据共享保密协议》（附件2），经相关数据归口管理部门审核同意后，信息中心根据数据处理工作量大小，在5—15个工作日内通过数据接口或数据导出等形式提供数据。对不符合技术规范的或影响学校数据安全的或以个人（含项目组）名义申请使用数据的，信息中心不予提供数据。对技术条件限制等，无法按指定规格提供数据的，信息中心应及时反馈申请部门。

第二十条 使用单位依据职能获得的共享数据仅限内部使用，如需对外提供或发布，应当向学校网络安全和信息化工作领导小组提出申请，经同意后方可对外提供或发布。

第二十一条 使用单位不得超出申请范围使用共享数据，

不得以任何方式用于社会有偿服务或其他商业活动，并对共享数据的滥用、非授权使用、未经许可的扩散以及泄露等行为及后果承担相应责任。

第七章　数据安全

第二十二条　学校网络安全和信息化工作领导小组组长为学校数据安全第一责任人，各信息系统主管部门负责人为直接责任人。

第二十三条　信息中心负责落实网络安全和信息化工作领导小组关于信息系统数据安全管理的业务指导意见，协调数据管理全过程的安全保障工作，防止未经授权的数据活动，开展信息系统数据安全风险评估、安全管理审查、安全质量考核及安全宣传教育，推进常态化数据安全监管机制,建立学校数据中心数据安全日志审计机制，运用高危操作监测与预警技术，及时对发现的违规行为进行核实处置，建立《数据安全事件应急预案》（附件 3），定期开展应急演练。按照信息安全等级保护要求，建立相应的安全管理技术方案，并负责学校数据中心安全的软硬件建设，逐步建立数据容灾备份中心，为信息系统数据安全管理提供系统支撑。

第二十四条　各信息系统管理部门应建立和严格执行信息系统安全运行、数据维护流程等制度，明确责任人，开展数据风险评估，落实安全管理责任制，按照网络安全等级保护制度，从技术和管理的各个层面执行数据安全管理制度，提高防病毒、

防攻击、防篡改、防泄露、防窃取等防护能力。定期开展数据安全检查并做好检查记录，配合开展网络信息安全漏洞排查工作。建立数据访问权限运行管理机制，做好数据访问账号权限分配、开通、使用、变更、重置、锁定、注销等申请审批、执行和记录工作，严格落实数据访问权限的时效性管理，加强高风险数据操作权限管理。信息系统应保留至少六个月的日志信息，信息系统的所有操作都要作为日志信息予以存储。日志信息的访问只能被授权的对象只读访问，任何人不得修改。

第二十五条 数据使用单位应当遵守有关保密和权益维护的法律法规和学校制度，承担下发数据的安全保障责任，落实使用完毕的数据清理和销毁工作，发现违规违法问题应及时报告有关部门依法依规处置。

第二十六条 只有相关法律法规和学校制度有明确规定需要公开的个人信息，方可进行公开。涉及个人信息的数据活动中，相关主体具有知情、决定、查询、更正、删除等权利。个人信息处理应当遵循合法、正当、必要、诚信的原则，按照“告知—同意”规则，在事先充分告知的前提下取得个人同意。公开个人信息遵循最小化原则，严禁超范围公开其他相关信息。

第二十七条 建立健全数据脱敏脱密处理机制，确需在非密环境下使用的涉及国家安全、社会公共利益、商业秘密、个人信息的数据依法进行脱敏脱密处理。

第二十八条 学校严格信息网络安全管理制度，定期排查

学校各类网络信息安全漏洞。对存在高风险网络信息安全漏洞的网站或系统，信息中心有权关闭相应网站或系统，以确保信息系统数据安全。

第二十九条 各信息系统后台管理权限配置，应严格按照“按需够用”原则进行授权，确保管理用户仅限查阅或操作与岗位职责相关的数据和业务。各部门使用信息系统数据时，应加强数据管理和使用人员的信息安全教育，应注意保护师生个人隐私和学校业务数据。未经批准，任何单位和个人不得擅自将获得的数据公开、转给他人使用或用于申请授权范围以外的用途。业务部门因开发对接需要，把数据接口密钥信息交给第三方时，必须与第三方签订网络安全保障与信息保密协议。

第三十条 注销的信息化系统或报废的存储设备，应确保承载的信息数据被彻底或有效删除且无法通过任何手段恢复，方可进行注销或报废处理。

第八章 数据管理监督

第三十一条 各部门及个人违反本办法规定，有下列情形之一的，由信息中心根据实际情况责令限期改正。造成严重不良后果的，按照相关规定予以追责：

1.未按规定开放或使用数据的；

2.提供数据目录和数据内容的质量不达标的，或未按照规定时限发布、更新数据目录和数据内容的；

3.数据使用管理失控，致使出现滥用、盗用及泄漏的；

4.未经授权，擅自将学校数据用于本部门履行职责所需范围以外的，或擅自转让给第三方的，或利用学校数据开展经营性活动的；

5.封锁、瞒报数据安全事件，拒不配合有关部门依法开展调查、处置工作，或者对有关部门通报的问题和风险隐患不及时整改并造成严重后果的。

第三十二条 对于违反法律、法规和学校相关规定，造成国家、学校和个人损失的，学校将依法依规追究相关单位及个人的责任。

第九章 附则

第三十三条 本办法自印发之日起开始施行，由信息中心负责解释，原《杭州师范大学信息系统数据管理办法》（杭师大发〔2017〕43号）同时废止。

附件 1

杭州师范大学信息系统数据使用审批单

申请部门		经办人姓名、工号及联系方式	
使用目的	使用目的说明： （为更好了解用户数据需求，请在本栏目详细描述数据使用情况及目的等信息）		
数据使用需求说明			
数据集名称	□教师类 □学生类 □教学类 □科研类 □财务类 □资产类 □系统数据类 □其他类		
字 段	(针对教师数据，包括工号、姓名、学院、职称等；针对学生数据，包括学号、姓名、学院、班级等，可提供数据格式样本)		
数据取得形式	□Excel 文件 □数据库同步（同步系统名称：_____）		
其他要求			
经办人签字	我严格遵守《杭州师范大学数据共享保密协议》。 数据使用经办人（签字）： 年 月 日		
部门审核意见	我部门保证监督数据使用者按照保密协议要求使用数据。 部门负责人（签字）： 部门（盖章） 年 月 日		

数据归口管理部门审核意见	
部门 1	□同意　□不同意，理由： 部门负责人签字（盖章）：　　年　　月　　日
部门 2	□同意　□不同意，理由： 部门负责人签字（盖章）：　　年　　月　　日
部门 3	□同意　□不同意，理由： 部门负责人签字（盖章）：　　年　　月　　日
数据技术支撑部门意见	
信息中心意见	□同意。上述数据归口管理部门审核后，信息中心根据数据量大小 5-15 个工作日提供数据。 □不同意，理由： □数据经办人不是我校在职教职工 □数据中心尚无所需数据 □所需数据不完整，请向数据归口部门索取 □数据需求范围过大，不符合“按需够用”原则 □其他原因： 负责人签字（盖章）： 年　　月　　日
备　注	

备注：本表一式两份，正反打印并盖章后，交信息中心，由信息中心统一至相关部门审批。

附件 2

杭州师范大学数据共享保密协议

为加强对学校数据中心共享数据的安全管理，根据《杭州师范大学信息系统数据管理办法》及有关规定制定本协议。

1.数据使用申请部门仅限杭州师范大学下属部门及学院，使用部门的行政主要负责人为数据安全的第一责任人，数据使用经办人负责数据安全管理。数据使用经办人必须为本校教职工。

2.使用部门必须遵守国家有关法律、行政法规和安全保密制度的规定。不得从事危害国家安全、泄露国家机密等违法犯罪活动；不得侵犯国家的、社会的、集体的利益和公民的合法权益。

3.使用部门对数据中心提供的数据，只享有使用权和数据提供权，数据的所有权归学校所有。委托第三方开发的应用系统使用本数据时，使用部门应和该公司签署数据安全保密协议。

4.使用部门不得有偿或无偿转让其从数据中心获得的数据，包括用户对这些数据进行换算、介质转换或者量度变换后形成的新数据。

5.使用部门不得将其从数据中心获得的数据向外分发，或用作向外分发或供外部使用的数据库、产品和服务的一部分，

也不得间接用作生成它们的基础。

6.使用部门从数据中心获得的数据用途必须与数据使用申请中规定的一致，需要改变用途时必须重新申请。

7.使用部门对所获得的数据的使用和保管，应严格遵照《中华人民共和国保守国家秘密法》关于保密制度的要求执行。

8.使用部门从数据中心获得的数据在相应业务信息系统上使用时，若业务系统出现危害数据安全的网络信息安全漏洞时，信息中心有权停止数据提供、关停相关业务信息系统，直至使用部门修复漏洞。

9.提供的数据来自于学校相关职能部门业务系统，信息中心无法承诺数据完全准确、齐全等数据质量。

10.对于没有遵守法律、法规及上述规定的，造成学校或师生信息泄露的，由有关部门依照法律、法规及学校规章对当事人进行处罚。

信息中心负责人：　　使用部门行政主要负责人：

日期：　　日期：

附件 3：

杭州师范大学网络安全保障与信息保密协议

甲方：杭州师范大学

乙方：_____

因乙方将为甲方提供_____服务，为切实保障甲方的网络和信息安全，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》及《杭州师范大学网络与信息安全管理办法》《杭州师范大学信息系统数据管理办法》等有关法律、规章之规定，为确保乙方为甲方提供信息化建设相关的项目开发维护服务所涉及的国家秘密和单位工作秘密的安全，甲、乙双方本着平等、自愿、公平和诚实信用的原则签订本协议。

第一条　保密范围

1.乙方为甲方提供信息化建设服务所涉及的合同、协议或存在事实合作、服务关系的项目开发、维护工程活动（以下简称服务工程）。

2.乙方为服务甲方的信息化建设而了解、掌握的甲方文件、资料、档案、各类业务运行信息、师生身份隐私信息、各类规划、顶层设计以及甲方专属局域信息网络系统的拓扑结构、安全保密措施、各项参数、场地环境、硬件、软件、信息系统数据、商业资料等所有资料内容（以下简称专有信息）。

3.甲方依照法律规定(如在缔约过程中知悉其他相对人的

商业秘密)和在有关协议的约定(如技术合同)中对外承担保密义务的事项，也属本保密协议所称的专有信息秘密。

第二条　网络安全保障和信息保密义务人

乙方为本协议所称的网络安全保障和信息保密义务人（以下简称义务人)，是指为甲方提供相关服务而使用甲方网络，或知悉甲方专有信息的人员。

义务人同意为甲方利益尽最佳努力，在履行职务期间不组织、参加或计划组织、参加任何竞争企业，或从事任何不正当使用商业和师生身份等其他信息秘密的行为。

第三条　全与保密责任

1.甲方应加强对乙方及其参与本服务工程的员工的安全保密监管，及时发现安全保密隐患和问题。乙方应配合甲方对乙方有关人员进行审查、教育培训，及时调整不合适的人员。

2.乙方必须在签定本保密协议后，才可使用甲方提供的有关专有信息，为甲方提供信息化建设相关项目的开发维护服务。

3.乙方使用甲方提供的网络或信息，应当遵守国家宪法法律，遵守公共秩序，尊重社会公德，遵守学校相关规章制度，自觉维护甲方的网络与信息系统安全，不得利用甲方网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动；不得发布、组

织或实施任何违法犯罪活动；不得发送垃圾邮件、传播计算机病毒，危害网络信息安全等。

4.乙方对其因身份、职务、职业或技术关系而知悉的甲方专有信息秘密应严格保守，保证不被披露或使用，包括意外或过失。即使这些信息甚至可能是全部由乙方因工作构思或取得的。

5.乙方同意严格控制使用甲方的专有信息，保证不向第三方泄露甲方提供的任何专有信息，并对该专有信息的管理提供良好的安全保密措施。

6.建设涉及数据库、网络、服务器等信息系统，乙方须制定甲方认可的安全保密管理方案，满足学校规定及信息安全等级保护二级及以上的要求，有效保障信息系统安全。

（1）主机及系统安全

乙方在项目实施中产生的账户，包括但不仅限于操作系统、数据库、应用系统后台等，系统密码不得使用简单密码及出厂默认密码，均应该设置为强密码，不能出现任何形式的弱密码，每季度至少更新一次密码。

乙方实施的服务工程中的操作系统和重要终端设备应安装实时检测和查杀恶意代码的软件产品，禁止在服务器中随意安装非官方的有安全风险的软件。

服务器安装部署后需开启系统防火墙，仅允许必要端口通过，乙方的所有主机维护操作需通过甲方的堡垒机完成。

定期安装系统的最新补丁程序，并根据厂家提供的可能危

害计算机的漏洞进行及时修补，并在安装系统补丁前对现有的重要文件进行备份。定期进行系统漏洞扫描，对发现的系统安全漏洞进行及时的修补。

实现应用系统特权用户的权限分离，根据业务需求和系统安全分析确定系统的访问控制策略，对系统账户进行分类管理，权限设定应当遵循最小授权要求。

（2）数据安全及备份恢复

数据完整性。能够检测到系统管理数据、鉴别信息和用户数据在传输过程中完整性受到破坏；能够检测到系统管理数据、鉴别信息和用户数据在存储过程中完整性受到破坏。

数据保密性。网络设备、操作系统、数据库管理系统和应用系统的鉴别信息、敏感的系统管理数据和敏感的用户数据应采用加密或其他有效措施实现传输保密性；当使用便携式和移动式设备时，应加密或者采用可移动磁盘存储敏感信息。

备份与恢复管理。识别需要定期备份的重要业务信息、系统数据及软件系统等；规定备份信息的备份方式(如增量备份或全备份等)、备份频度(如每日或每周等)、存储介质、保存期等；根据数据的重要性和数据对系统运行的影响，制定数据的备份策略和恢复策略，备份策略应指明备份数据的放置场所、文件命名规则、介质替换频率和将数据离站运输的方法；指定相应的负责人定期维护和检查备份及冗余设备的状况，确保需要接入系统时能够正常运行；根据备份方式，规定相应设备的安装、配置和启动的流程。

（3）安全事件处置

分析信息系统的类型、网络连接特点和信息系统用户特点，了解本系统和同类系统已发生的安全事件，识别本系统需要防止发生的安全事件，记录并保存所有报告的安全弱点和可疑事件，分析事件原因，监督事态发展，采取措施避免安全事件发生。

发现有造成安全事件，或专有信息秘密被泄露或者自己过失泄露事件，乙方应当采取有效措施防止事件及后果进一步扩大，并及时向甲方报告，尽最大可能消除影响，并应承担全部法律责任。

（4）应急预案管理

在甲方的应急预案框架下制定不同事件的应急预案，应急预案框架应包括启动应急预案的条件、应急处理流程、系统恢复流程和事后教育和培训等内容；对系统相关的人员进行培训使之了解如何及何时使用应急预案中的控制手段及恢复策略，对应急预案的培训至少每年举办一次。

7.乙方不得将甲方的专有信息用于未经甲方书面许可的其它任何目的。除乙方直接参与本服务工程的职员之外，不得将专有信息透露给其它任何人。乙方及其参与本服务工程的员工严禁在系统建设中私设“后门”，非法访问系统或转移、加工系统数据。乙方应当告知并采取有效措施要求其参与本服务工程的员工遵守本协议规定。

8.乙方发现保密范围内的有关事项已经泄露或可能泄露时

应当及时报告甲方，并无条件立即采取相应补救措施。

9.当甲方以书面形式要求乙方交回专有信息时，乙方应当立即交回所有书面的或其他形式的专有信息以及所有描述和概括该专有信息的文件资料，不能以任何形式保留或擅自处理。

10.乙方因不可抗力（如法律、法规、国家政策调整等）而透露信息或向第三方提供信息系统资料的，应当事先书面通知甲方，并且尽力提供保护。

11.未经甲方许可，乙方不得带走从甲方得到的任何文档、图纸、资料、磁盘（含U盘）、胶片等载有甲方秘密信息的介质，以及甲方用户数据。当本合同项目结束时，乙方应将需要保存的甲方资料及其复印件的保存清单交给甲方，并由甲方确认，其他资料不得擅自保留。更不能上传至互联网。

12.乙方在项目建设及服务过程中，应确保项目文档由专人负责保管，确保项目文档的使用受到控制，甲方提供给乙方的保密信息，乙方应指定专人接收、登记、返还。

13.乙方工作人员离岗时，乙方需办理严格的手续，承诺调离后的保密义务方可离开，离岗后应立即终止离岗员工的所有访问权限，取回各类与甲方相关的软硬件设备。

第四条　违约责任

1.义务人违反协议中的义务，应承担违约责任。

2.乙方如危害甲方网络安全，或将商业和师生身份等其他信息秘密泄露给第三人，涉及违法的，报送公安机关进行处理，不涉及违法，但使甲方遭受损失的，乙方应对甲方进行赔偿，

其赔偿金额不少于由于其违反义务所给甲方带来的损失。

3.因乙方的违约或侵权行为侵犯了甲方的网络安全、商业和师生身份等其他信息秘密权利的，甲方可以选择根据本协议要求乙方承担违约责任，或者根据国家有关法律、法规要求乙方承担侵权责任。

4.因乙方恶意破坏甲方网络安全、泄露商业和师生身份等其他信息秘密造成严重后果的，甲方将通过法律手段追究其侵权责任，直至追究其刑事责任。

签署本协议前，双方已经详细审阅了协议的内容，并完全了解协议各条款的法律含义。

本协议自双方签字或盖章后生效。

本协议甲乙双方各执一份，乙方参与人员各执一份。

甲方（盖章）：杭州师范大学

联系人：

乙方（盖章）：

乙方法定代表人或委托代理人签字：

年　　月　　日

乙方参与人员

姓名	身份证号	工作内容	是否已知悉保密协议内容并承诺遵守	本人签字

附件 4

杭州师范大学数据安全事件应急预案

为提高我校处置数据安全事件的能力，形成科学、有效、反应迅速的应急工作机制，最大程度预防和减少数据安全突发事件及其造成的损害，增强对突发事件的应变能力，并使应急工作安全、有序、科学、高效地实施，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》《网络数据安全管理条例（征求意见稿)》《信息安全事件分类分级指南》(GB/T20986-2007）等国家有关法律法规，结合学校工作实际，特制定本预案。

第一章　总则

第一条　安全事件定义。数据安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等原因，学校各系统内数据资产的可用性、保密性、完整性被破坏，以及数据被违规收集、使用、处理，数据被违规出售、转移，数据超期留存等，数据泄露（丢失)、滥用、被篡改、被损毁、违规使用，对学校及师生个人工作、学习、生活秩序、社会声誉造成负面影响，需要采取应急处置措施予以应对的数据安全突发事件。

第二条　适用范围。本预案适用于我校各单位发生的数据安全事件的报告与处置工作。

第三条 工作原则。坚持预防为主、预防与应急相结合的原则，坚持“谁主管谁负责、谁运行谁负责”的原则，充分发挥各方面力量共同做好数据安全事件的预防和处置工作。

第二章 组织机构与职责

第四条 学校网络安全和信息化工作领导小组统一领导全校数据安全应急工作，领导小组在数据安全工作领域主要职责如下：

1.研究制订学校数据安全应急处置工作的规划和政策，协调推进学校数据安全应急机制和工作体系建设；

2.检查、指导和督促数据安全应急机制建设，指导督促数据安全应急预案的修订和完善，检查落实预案执行情况；

3.统筹学校各类数据安全突发事件的组织和协调工作；

4.对数据安全突发事件相关信息进行及时收集和分析，组织重大事件的研判、调查、处置和总结评估工作。

第五条 领导小组主要成员工作职责。

（一）学校办公室

牵头组织活动、重要会议期间发生的数据安全事件的协调处置和预警意见；负责涉密级信息数据泄密类事件的处理。

（二）信息中心

负责监测、报告数据安全突发事件和预警信息；负责突发数据安全事件学校中心机房服务器端和网络层面的技术处置与调度工作；成立应急办公室，负责数据安全事件日常管理工作，

开通咨询电话，为学校各单位的数据安全事件应急处置提供技术指导，对各单位信息员进行培训。

（三）党委宣传部

负责学校舆情监测和内容发布类系统数据篡改事件的处置工作；对于涉及师生思想政治方面的预警性、倾向性、苗头性问题进行分析研判；对于校内危害国家安全、社会稳定和学校正常教学秩序的信息，以及校外恶意诋毁或虚假报道我校的信息，负责会同有关部门及时清理或正面回复，进行网络舆情正面引导。

（四）保卫处

密切联系公安部门，负责涉及人为破坏类事件的应急处置；配合完成重大数据安全事件的应急处置工作；对于触犯法律法规及学校规章制度行为追究相关责任。

（五）后勤中心

负责数据安全事件应急处置的后勤保障工作，主要包括电力保障、交通保障、场地保障等。

（六）计划财务处

负责数据安全事件应急处置所需的物资采购经费等。

第六条 各学院、部门负责本单位业务系统的数据安全事件的处置工作，应对照本预案，建立本单位应急处置机制。

第三章 事件分级和分类

第七条 数据安全事件分为四级：特别重大数据安全事件

（Ⅰ级）、重大数据安全事件（Ⅱ级）、较大数据安全事件（Ⅲ级）、一般数据安全事件（Ⅳ级），Ⅰ级为最高级。

（一）特别重大数据安全事件（Ⅰ级）

重大事件是指能够导致特别严重影响或破坏的数据安全事件，包括以下情况：

1.对外提供服务的网站类应用系统，其页面被篡改为反动信息、煽动性信息等造成严重政治影响的；

2.重要敏感信息和关键数据丢失或被窃取、篡改、假冒，产生特别重大的社会影响；

3.发生特别重大数据泄露事件，造成5万条以上数据泄露的；

4.其他造成特别重大损失或特别重大的不良影响的安全事件。

（二）重大数据安全事件（Ⅱ级）

重大事件是指能够导致严重影响或破坏的信息安全事件，包括以下情况：

1.重要敏感信息和关键数据丢失或被窃取、篡改、假冒，产生重大的社会影响；

2.发生重大数据泄露事件，造成5万条以下5千条及以上数据泄露的。

3.其他造成或可能造成重大危害或影响的数据安全事件。

（三）较大数据安全事件（Ⅲ级）

较大事件是指能够导致较大范围影响或破坏的数据安全事件，包括以下情况：

1.对外提供服务的网站类应用系统其页面被篡改，发布虚假或诈骗等信息并已造成较大的经济和社会影响；

2.重要敏感信息和关键数据丢失或被窃取、篡改、假冒，产生较大的社会影响；

3.发生较大数据泄露事件，造成5千条以下50条及以上数据泄露的。

4.其他造成或可能造成较大危害或影响的数据安全事件。

（四）一般数据安全事件（Ⅳ级）

一般事件是指能够导致轻微影响或破坏的网络安全事件，包括以下情况：

1.重要敏感信息和关键数据丢失或被窃取、篡改、假冒，产生一般的社会影响；

2.发生一般数据泄露事件，造成50条及以下数据泄露的；

3.其他造成或可能造成一般危害或影响的数据安全事件。

第八条 综合考虑数据安全事件的起因、表现、结果等，数据安全事件可分为数据泄露（丢失）、数据篡改、数据损毁、数据滥用违规使用和其它数据破坏事件。

1.数据泄漏（丢失）事件是指因误操作、人为蓄意、软硬件缺陷或电磁泄漏等因素导致网络、系统、平台中的保密、敏感、个人隐私等重要数据暴露于未经授权者，而导致的数据安

全事件。

2.数据篡改事件是指未经授权将网络、系统、平台中的数据更换为攻击者所提供的数据而导致的数据安全事件。

3.数据被损毁事件是指因误操作、人为蓄意、软硬件缺陷、外围保障设施故障、人为破坏事故和其它设备设施故障、自然灾害等因素导致网络、系统、平台的数据删除、乱码、数据完整性破坏、数据存储介质销毁等数据安全事件。

4.数据滥用违规使用事件是指数据使用方胡乱或超范围收集、使用数据，或在数据使用的过程中违反学校规定及相关国家法律法规或条例而导致的数据安全事件。

5.其它数据安全事件是指不能被包含在以上分类之中的安全事件。

学校各单位一旦发生数据安全事件，应根据数据安全事件分类分级方法，视数据重要程度、损失情况以及对工作和社会造成的影响迅速自主判定安全事件等级。应急办公室在接到报告后，根据事件情况，进一步作出判定。必要时，应急办公室组织专家组进行判定或报告学校网络安全和信息化工作领导小组判定。

第四章　预防措施

第九条　建立健全数据安全治理体系，提高数据安全保障能力，建立预报预警监测体系，及时采取有效措施，减少和避免数据安全事件的发生及危害，提高应对数据安全事件的能力。

第十条 健全技术防护体系，在校园网出入口、数据中心、重要信息系统等重要部位，安装必要的安全防御检测工具和日志审计系统，进行实时监测和定期扫描，做好数据安全的日常巡查工作，发现数据安全缺陷、漏洞等风险时，应当立即采取补救措施，党委宣传部及各信息员应监控学校网站内容，发现异常情况及时防范处理并逐级报告。信息员做好各单位数据备份、系统升级、定期杀毒等日常管理，并按《网络与信息安全日常维护登记表》（附件4.1）做好相应登记。

第十一条 加强宣传和培训，充分利用各种传播媒介及其他有效的宣传形式，加强数据安全事件预防和处置的有关法律、法规和政策的宣传，开展数据安全基本知识和技能的宣传活动，提高全体人员的应急意识和应急基本常识。

第十二条 定期开展应急演练，检验和完善预案，提高实战能力，每年至少组织一次预案演练，以检验应急预案的正确性，不断加强人员的应急安全意识和应急响应的熟练程度。

第十三条 应急领导小组统筹协调重要活动期间数据安全保障工作，要求各应急工作小组在重要活动期间进一步加强数据安全监测和分析研判，加强数据安全事件的防范和应急响应，其中，核心网络和重要信息系统的重点岗位应保持24小时值班，及时发现和处置数据安全事件隐患。

第五章 报告与处置

第十四条 Ⅰ至Ⅲ级数据安全事件的报告与处置分为三个

步骤：事发紧急报告与处置、事中情况报告与处置和事后整改报告与处置。

（一）事发紧急报告与处置

1.发生数据安全事件后，涉事单位应第一时间采取断网等有效措施进行处置，将损害和影响降到最小范围，保留现场，并报告本单位安全责任人和主要负责人。

2.本单位安全责任人接到报告后，应立即组织相关人员赶赴现场进行紧急处置，同时以口头通讯的方式将相关情况通报至信息中心及相关部门，并书面记录安全事件发现过程及口头汇报过程。涉及人为主观破坏事件应同时报告保卫处。

3.信息中心接到报告后，应做好书面记录，并进一步判定安全事件等级，对确认属Ⅰ至Ⅲ级安全事件的，应报告领导小组副组长，根据情况需要报组长。

4.紧急报告内容包括：时间地点、简要经过、事件类型与分级、影响范围、危害程度、初步原因分析、已采取的应急措施。

5.对确认属Ⅰ至Ⅲ级安全事件的，应急办公室应立即组织相关技术力量赶赴现场进行协助处置工作。涉及人为主观恶意事件的，保卫处应组织人员赴现场协助处置，并协助公安机关做好相关取证和处置工作。

6.各单位应及时跟进事件发展情况，出现新的重大情况应及时补报。

（二）事中情况报告与处置

1.事中情况报告应在安全事件发现后 5 小时内以书面报告的形式进行报送，报送内容和格式见附件 4.2。

2.事中情况报告由单位安全负责人组织编写，由本单位主要负责人审核后，签字并加盖公章报送应急办公室。涉及人为主观破坏事件的，事中情况报告应抄送给保卫处。

3.数据安全事件应急处理过程中根据不同事件类型采取以下应急处理措施：

（1）数据泄露（丢失）事件

在发生数据泄露安全事件后，应准确评估泄露的数据，视风险高低决定是否暂停系统服务。保护与泄露相关的物理区域，保留与数据泄露相关的一切记录，待取证分析专家和执法人员查证，及时封堵数据泄露源头，彻查潜在的安全漏洞，一旦发现立即处置。查找任何已经泄露的数据，采取必要措施将这些数据从各类传播媒介中删除，降低数据泄露事件的影响，视事件严重程度由保卫处联系、配合公安部门开展调查，对组织剽窃、盗走或使用学校数据的违法人员进行追责。

（2）数据被篡改事件

在发生数据被篡改安全事件后，可采取暂时切断网站对外服务，网站维护人员即刻登录后台，上传换回原始页面，或对数据进行完整性校验，从备份数据对被篡改的数据进行恢复，安全监控平台随时密切监视信息内容，保存有关日志审计记录，

备份不良信息出现的目录，降低数据被篡改事件的影响，视事件严重程度由保卫处联系、配合公安部门开展调查，对通过非法途径对学校数据进行篡改的行为进行追责。

（3）数据损毁事件

及时从备份数据中恢复受破坏的最新信息数据，检查恢复后的系统状态是否正常运行，分析信息数据受破坏的原因，系统故障导致的应分析系统软件故障点，及时联系软件开发商进行修复；硬件设备故障的，及时切换备用设备；涉及人为主观破坏的损毁事件应由保卫处联系、配合公安部门开展调查；遇到自然灾害，受灾机房网络及信息系统受破坏不能提供服务的，应及时启用容灾机房备份数据。

（4）数据滥用、违规使用事件

在发生数据滥用、违规使用安全事件后，要求有关组织、个人采取措施进行整改，消除影响，并视事件严重程度由保卫处联系、配合公安部门开展调查，对滥用、违规使用学校数据的违法组织、个人进行追责。

（三）事后整改报告与处置

1.事后整改报告应在安全事件处置完毕后 4 个工作日内以书面报告的形式进行报送，报送内容和格式见附件 4.3。

2.事后情况报告由单位安全负责人组织编写，由本单位主要负责人审核后，签字并加盖公章报送应急办公室。

3.安全事件事后处置包括：进一步总结事件教训、研判安

全现状、排查安全隐患、进一步加强制度建设、提升安全防护能力。如涉及人为主观破坏的安全事件应继续配合公安部门和保卫处开展调查。

第十五条 一般安全事件（Ⅳ级）报告与处置。各单位发生一般安全事件，应及时、自主组织应急处置工作；需要应急办公室协助的，可联系予以协助。在事件处置完毕后 6 天内向应急办公室报送整改报告，报告内容和格式见附件 4.3。

第六章 保障措施

第十六条 为保障联络通畅，各单位的信息安全工作主管领导、信息员联络方式发生变更的，应填写《应急信息员队伍汇总表》（附件 4.4），及时向应急办公室报备。

第十七条 各单位应根据实际建立本单位的值守制度，做到安全事件早预警、早发现、早报告、早控制、早解决。各单位应建立健全本单位安全事件应急处置机制，制定安全事件应急预案，定期组织应急演练。

第十八条 信息中心应根据数据安全应急处置工作实际需要，提出用于安全的软硬件设备及运行维护经费预算，报计划财务处纳入年度经费预算，以专项经费列支。

第十九条 各单位应按照预案及时、如实地报告和妥善处置安全事件。如有瞒报、缓报、处置和整改不力等情况，学校将对相关单位进行约谈或通报；情况严重的将进行问责处理。

第七章 附则

第二十条 本预案自印发之日起施行，由网络安全和信息化工作领导小组办公室负责解释。

附件：4.1 网络与信息安全日常维护登记表

4.2 杭州师范大学数据安全事件情况报告

4.3 杭州师范大学数据安全事件整改报告

4.4 应急信息员队伍汇总表

附件 4.1

网络与信息安全日常维护登记表

单位名称（公章）：　　报送时间：　　年　　月　　日

维护日期	实施人	维护内容				备注
		运行情况	数据备份	病毒查杀	补丁更新	

附件 4.2

杭州师范大学数据安全事件情况报告

单位名称(公章)：　　事发时间：　　年　月　日　时　分

<table>
<tr><td rowspan="2">联系人
姓　名</td><td rowspan="2"></td><td>联系电话</td><td></td></tr>
<tr><td>电子邮箱</td><td></td></tr>
<tr><td>事件分类</td><td colspan="3">口 数据泄露（丢失）事件　　口 数据篡改事件
口 数据损毁事件　　口 数据滥用违规使用故障
口 其他</td></tr>
<tr><td>事件分级</td><td colspan="3">口Ⅰ级　口Ⅱ级　口Ⅲ级　口Ⅳ级</td></tr>
<tr><td>事件概况</td><td colspan="3"></td></tr>
<tr><td>信息系统基本情况（如涉及请填写）</td><td colspan="3">1.系统名称：
2.系统网址和 IP 地址：
3.系统主管单位/部门：
4.系统运维单位/部门：
5.系统使用单位/部门：
6.系统主要用途：
7.是否定级：　口是　口否，所定级别：
8.是否备案：　口是　口否，备案号：
9.是否测评：　口是　口否
10.是否整改：　口是　口否</td></tr>
</table>

事件发现与处置的简要经过	
事件初步估计的危害和影响	
事件原因初步分析	
已采取的应急措施	
是否需要应急支援及需支援事　项	
直　接责任人意　见	签名：　　年　月　日
第　一负责人意　见	签名：　　年　月　日

附件 4.3

杭州师范大学数据安全事件整改报告

单位名称(公章)：　　事发时间：　　年　月　日　时　分

<table>
<tr><td rowspan="2">联系人
姓　名</td><td rowspan="2"></td><td>联系电话</td><td></td></tr>
<tr><td>电子邮箱</td><td></td></tr>
<tr><td>事件分类</td><td colspan="3">口 数据泄露（丢失）事件　　口 数据篡改事件
口 数据损毁事件　　口 数据滥用违规使用故障
口 其他</td></tr>
<tr><td>事件分级</td><td colspan="3">口Ⅰ级　口Ⅱ级　口Ⅲ级　口Ⅳ级</td></tr>
<tr><td>事件概况</td><td colspan="3"></td></tr>
<tr><td>信息系统基本情况（如涉及请填写）</td><td colspan="3">1.系统名称：
2.系统网址和 IP 地址：
3.系统主管单位/部门：
4.系统运维单位/部门：
5.系统使用单位/部门：
6.系统主要用途：
7.是否定级：　口是　口否,所定级别:
8.是否备案：　口是　口否,备案号:
9.是否测评：　口是　口否
10.是否整改：　口是　口否</td></tr>
</table>

事件发生的最终判定原因（可加页附文字、图片以及其他文件）	
事件的影响与恢复情　况	
事件的安全整改措施	
存在问题及建议	
是否需要应急支援及需支援事　项	
直　接责任人意　见	签名：　　年　月　日
第　一负责人意　见	签名：　　年　月　日

附件 4.4

应急信息员队伍汇总表

单位名称（公章）：　　报送时间：　　年　月　日

序号	姓名	性别	单位	信息职责	联系方式 （移动电话）

主送：各学院（部）、部门。

杭州师范大学校长办公室　　2023 年 5 月 31 日印发