# An Electroencephalogram Dataset of Learner Interest States in Online Education Tasks 数据保存政策

1. 总则

1.1 政策目的

1.1 政策目的

为规范“在线教育任务中学习者兴趣状态的脑电图数据集”（以下简称“本数据集”）的数据保存管理，重点保障脑电图（EEG）生物识别数据的隐私安全与学术研究数据的完整性、可追溯性，明确数据在采集、预处理、存储、备份、归档、销毁等全生命周期的保存要求，维护学习者（数据主体）的合法权益，支撑在线教育心理学、神经教育学等领域的学术研究与成果转化，依据《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》《人类遗传资源管理条例》及学术研究伦理规范，制定本政策。

1.2 适用范围

1.2 适用范围

本政策适用于本数据集所有数据的产生、采集、预处理、标注、存储、备份、归档、检索、学术使用及销毁等各环节的管理活动，覆盖数据集建设单位、数据采集团队、标注人员、运维技术人员、学术使用方及外部合作机构（如伦理审查委员会、云存储服务商）。本政策所指数据包括：EEG 原始信号数据、EEG 预处理数据（如去噪、滤波后数据）、学习者基本信息（已去标识化处理）、在线教育任务场景数据（如任务类型、难度、时长）、兴趣状态标注数据（如专家标注结果、算法预测结果）、实验伦理审查文件、数据采集知情同意书扫描件及系统运维日志等结构化、半结构化及非结构化数据。

1.3 基本原则

1.3.1 合规性原则：严格遵循国家及地方相关法律法规、监管要求，确保数据保存活动合法合规，杜绝任何违反法律规定的数据处理行为。

1.3.2 安全优先原则：将数据安全作为核心目标，建立多层次、全方位的安全保障体系，防范数据泄露、丢失、篡改、损坏等风险，保障数据在全生命周期内的安全。

1.3.3 完整可用原则：采取必要的技术与管理措施，确保保存的数据内容完整、准确，能够满足业务开展、数据追溯及后续使用的需求，保障数据的长期可用性。

1.3.4 分类分级原则：根据数据的敏感程度、重要性、业务价值及合规要求，对数据进行分类分级管理，针对不同类别、级别的数据制定差异化的保存策略，提高管理效率与针对性。

1.3.5 权责明确原则：明确各部门、岗位在数据保存管理中的职责与权限，建立清晰的责任追溯机制，确保各项数据保存工作落到实处。

1.3.6 伦理合规原则：严格遵循学术研究伦理要求，所有数据处理活动均以获得数据主体有效知情同意为前提，严禁以任何形式泄露学习者身份信息，保障数据主体的知情权、删除权与更正权。

2. 数据分类与分级

2.1 数据分类
2.1 数据分类
结合本数据集“EEG 生物识别+教育场景”的核心特性，数据主要分为以下类别：
2.1.1 学习者生物识别与身份数据：包括 EEG 原始信号数据、EEG 特征提取数据等生物识别信息，以及经去标识化处理的学习者基本信息（如年龄、教育阶段，已剔除姓名、身份证号、学号等唯一标识）。
2.1.2 学术研究核心数据：支撑研究结论的关键数据，包括在线教育任务设计方案、学习者兴趣状态标注数据（含标注规则、标注人员资质信息）、数据预处理流程说明（含算法参数、去噪方法）、数据分析中间结果及研究成果关联数据。
2.1.3 实验与伦理管理数据：保障数据集合规性的支撑数据，包括伦理审查批件、学习者知情同意书（纸质扫描件或电子签名版）、数据采集设备校准记录、实验过程日志等。
2.1.4 系统运维数据：保障数据集存储与服务系统正常运行的数据，包括存储服务器配置信息、数据访问日志、运维操作记录、安全漏洞扫描报告、数据备份日志等。
2.1.5 公开学术信息数据：可对外公开的非敏感数据，包括数据集元数据（如数据规模、采集设备型号、任务类型说明）、学术论文引用信息、数据集使用规范说明等。
2.1.1 个人信息数据：包括用户姓名、身份证号、联系方式、住址、生物识别信息等能够识别特定自然人身份或反映特定自然人活动情况的各类信息。
2.1.2 业务核心数据：支撑数据库核心业务运行的数据，如交易记录、业务订单、服务协议、项目信息、成果数据等对业务开展具有关键作用的数据。
2.1.3 学术研究数据：与学术研究相关的原始数据、实验数据、分析报告、文献资料等数据，需满足学术规范及成果追溯要求。
2.1.4 系统运维数据：保障数据库系统正常运行的数据，包括系统配置信息、运行日志、监控数据、补丁记录、运维操作记录等。
2.1.5 公开信息数据：依法可以公开传播的信息，如公共服务公告、行业资讯、非敏感业务介绍等数据。
2.2 数据分级
2.2 数据分级
基于 EEG 数据的生物敏感性及学术研究价值，将数据划分为四个级别，分级标准及管理要求如下：
2.2.1 一级（极敏感生物数据）：EEG 原始信号数据、未完全去标识化的学习者生物特征关联数据。此类数据泄露可能导致学习者身份被精准识别，引发隐私侵犯、生物信息滥用等重大风险，且属于学术研究核心不可再生数据。
2.2.2 二级（高敏感研究数据）：EEG 预处理数据、兴趣状态标注原始数据、学习者知情同意书扫描件、伦理审查批件。此类数据虽经初步处理，但仍具备身份追溯可能性，且直接影响研究成果的真实性与可重复性。
2.2.3 三级（一般敏感数据）：去标识化后的学习者基本信息（如年龄区间、专业方向）、数据预处理流程说明、在线教育任务场景详情、数据访问申请记录。此类数据泄露对学习者权益影响较小，但需保障学术使用的规范性。
2.2.4 四级（非敏感学术数据）：数据集元数据（如数据量、采集时间范围、设备型号）、公开的学术引用信息、数据集使用规范、非敏感的实验场景图片或说明。此类数据可自由公开，无隐私安全风险。

2.2.1 一级（极敏感数据）：涉及国家秘密、核心商业秘密，或泄露后可能导致自然人合法权益受到严重损害、引发重大安全事件或造成重大经济损失的数据，如核心技术数据、未公开的重大决策数据、敏感个人生物识别信息等。
2.2.2 二级（高敏感数据）：涉及商业秘密、重要个人信息，泄露后可能导致自然人合法权益受到较大损害、引发较大安全风险或造成较大经济损失的数据，如用户完整身份证号、银行账户信息、重要业务合同数据等。
2.2.3 三级（一般敏感数据）：具有一定敏感性，泄露后可能导致自然人合法权益受到一定损害或引发一般安全风险的数据，如用户姓名、联系方式、普通业务记录等。
2.2.4 四级（非敏感数据）：公开或低敏感数据，泄露后对个人、组织及业务造成的影响极小的数据，如公开的行业资讯、非敏感的公共服务信息等。
3. 数据采集与录入保存要求
3.1 数据采集规范
3.1 数据采集规范
3.1.1 数据采集需以通过学术伦理审查为前置条件，严格遵循“合法、正当、必要”及“最小化采集”原则，仅采集与“学习者兴趣状态识别”直接相关的 EEG 数据及基础信息，不得采集与研究无关的生物特征或身份信息。对于学习者信息，需采用“去标识化优先”处理，采集后立即剔除姓名、学号、手机号等唯一标识，仅保留研究所需的分类信息。
3.1.2 采集前必须向学习者（或未成年学习者的监护人）提供书面知情同意书，明确告知数据采集目的、用途（仅限学术研究）、保存期限、数据安全保障措施及学习者的撤回同意权、数据删除权，经学习者签字确认后方可启动采集。知情同意书需单独归档保存，保存期限不短于数据本身保存期限。
3.1.3 EEG 数据采集需使用经计量校准的专业设备（如 NeuroScan、Emotiv 等合规设备），采集人员需具备相关操作资质，采集过程中实时记录设备参数、采集时间、学习者状态（如是否疲劳、是否配合）等信息，确保数据可追溯。采集的数据需即时存储至加密终端，避免在非加密设备中暂存。
3.1.4 对于合作单位提供的关联数据（如教育任务设计方案），需签订学术数据共享协议，明确数据使用范围、保密义务及知识产权归属，同时审核数据来源的伦理合规性，确保其符合本政策要求。
3.1.2 采集的数据需保证来源合法、内容真实、准确无误，采集过程需做好记录，包括采集时间、采集来源、采集人员、采集方式等信息，确保数据可追溯。
3.1.3 对于外部获取的数据，需与数据提供方签订合法的数据获取协议，明确双方的权利义务，确保数据获取及后续使用符合相关规定，并对数据来源及合法性进行审核验证。
3.2 数据录入要求
3.2.1 数据录入需指定专人负责，录入人员需经过专业培训，熟悉数据录入规范及相关操作流程。录入过程中需严格按照数据标准进行录入，避免出现错别字、格式错误、数据缺失等问题。
3.2.2 建立数据录入校验机制，对录入的数据进行实时校验，包括格式校验、逻辑校验、完整性校验等，发现错误及时修正。对于批量录入的数据，需在录入前进行样本测试，录入后进行全面核对。
3.2.3 数据录入完成后，需由专人进行审核确认，审核通过后方可正式存入数据库。审核记录需与数据一并保存，包括审核人员、审核时间、审核意见等信息。

4. 数据存储管理
4.1 存储介质选择
4.1 存储介质选择
4.1.1 基于数据敏感性分级采用差异化存储方案：一级数据需存储于物理隔离的加密服务器或合规的医疗健康级云存储服务（需通过等保三级及以上认证），采用“本地+异地”双活存储架构；二级数据可存储于企业级加密分布式存储系统，配备实时冗余备份；三级、四级数据可根据访问频率选择云存储或本地存储，但需确保存储介质的安全认证。
4.1.2 所有存储介质需符合国家信息安全标准，支持数据加密、访问日志审计等功能。严禁使用私人 U 盘、移动硬盘、非加密云盘（如个人百度云）等存储一级、二级数据；存储设备需指定专人管理，定期进行健康状态检测，避免因硬件故障导致数据丢失。
4.1.3 建立“数据-介质-责任人”关联台账，详细记录一级、二级数据的存储位置、介质编号、加密密钥责任人、数据写入时间等信息，每季度对台账进行核对更新，确保数据存储可追溯。
4.1.2 存储介质需符合国家相关标准，具备良好的稳定性、可靠性及可扩展性。禁止使用未经安全认证的存储设备，如私人 U 盘、移动硬盘等存储敏感数据。
4.1.3 建立存储介质管理台账，对存储介质的采购、分配、使用、维护、报废等情况进行全程记录，明确介质负责人及使用范围。
4.2 存储安全保障
4.2 存储安全保障
4.2.1 实施“全链路加密”策略：一级数据采用 AES-256 加密算法进行存储加密，数据传输过程采用 SSL/TLS 1.3 协议加密，加密密钥由双人分管，定期轮换；二级数据采用 SM4 加密算法，确保数据在存储和访问过程中不可被未授权获取。
4.2.2 建立“三重访问控制”机制：基于角色（RBAC）分配访问权限，一级数据仅向核心研究人员开放，且需“双人授权+动态密码”方可访问；二级数据需经项目负责人审批后授权访问；所有访问权限均设置有效期，到期自动回收。访问权限的申请、变更、撤销需留存纸质审批记录，与电子日志同步归档。
4.2.3 存储系统需部署“纵深防御”安全措施，包括防火墙、入侵防御系统（IPS）、终端安全管理系统（EDR）及数据防泄漏（DLP）工具，重点监控一级、二级数据的下载、复制行为。每月开展一次安全漏洞扫描，每半年开展一次渗透测试，及时修复安全隐患。
4.2.4 针对 EEG 数据的特殊性，建立“数据篡改实时监测”机制，对一级、二级数据的文件完整性进行哈希值校验，一旦发现数据被篡改立即触发告警并启用备份数据恢复，同时追溯篡改行为来源。
4.2.2 建立严格的存储系统访问控制机制，基于最小权限原则为不同岗位人员分配存储系统的访问权限，实现权限的精细化管理。访问权限的申请、变更、撤销需履行严格的审批流程，并做好记录。
4.2.3 存储系统需配备完善的安全防护措施，包括防火墙、入侵检测系统、防病毒软件等，定期进行安全漏洞扫描及风险评估，及时修复安全隐患，防止非法入侵、数据篡改等攻击行为。
4.2.4 定期对存储系统进行维护保养，包括硬件设备检修、软件系统升级、数据整理等工作，确保存储系统的稳定运行。维护过程需制定详细的操作方案，避免因维护操作不当导致数据丢失或损坏。

5. 数据备份与恢复
5.1 数据备份策略
5.1 数据备份策略
5.1.1 建立“分级备份+多副本”机制，结合 EEG 数据不可再生的特点，制定差异化备份方案：
（1）一级数据：采用“实时同步备份+每日全量备份+每 30 分钟增量备份”，生成 3 份副本（本地 1 份、同城异地 1 份、异地灾备 1 份），异地灾备距离不小于 300 公里，备份介质均采用加密存储；
（2）二级数据：采用“每日全量备份+每 2 小时增量备份”，生成 2 份副本（本地+异地），备份频率可根据数据更新量动态调整；
（3）三级数据：采用“每周全量备份+每日增量备份”，生成 1 份异地副本；
（4）四级数据：采用“每月全量备份”或按需备份，确保公开数据的可用性。
5.1.2 备份数据的加密级别与主数据一致，备份完成后需立即进行完整性校验，校验通过后方可确认备份有效。备份日志需详细记录备份时间、备份人员、数据量、校验结果等信息，与数据备份文件同步归档。
5.1.3 异地备份存储点需具备独立的安全防护体系，与主存储点实现物理隔离，避免因同一区域的自然灾害、电力故障等导致主备数据同时损坏。对于云备份服务，需选择具备跨区域灾备能力的服务商，并签订数据安全保障协议。
（1）一级数据：采用“实时备份+每日全量备份+每小时增量备份”的方式，确保数据的最小丢失量；
（2）二级数据：采用“每日全量备份+每两小时增量备份”的方式；
（3）三级数据：采用“每周全量备份+每日增量备份”的方式；
（4）四级数据：可根据实际需求采用“每月全量备份”或按需备份的方式。
5.1.2 备份数据需采用异地存储方式，主备份存储与异地备份存储之间的距离需符合安全要求，避免因自然灾害、区域性事故等导致主备数据同时损坏。异地备份可选择自有异地存储节点或合规的第三方存储服务。
5.1.3 备份数据需进行加密处理，备份介质或备份系统需具备与主存储系统同等的安全防护级别。同时，建立备份数据的标识体系，明确备份数据的名称、备份时间、数据级别、备份方式等信息，便于管理和检索。
5.2 备份验证与恢复
5.2.1 定期对备份数据进行验证，包括数据完整性验证、可用性验证等，确保备份数据能够正常恢复。一级、二级数据的备份验证频率不低于每月一次，三级、四级数据不低于每季度一次。验证记录需详细留存，包括验证时间、验证人员、验证方法、验证结果等信息。
5.2 备份验证与恢复
5.2.1 定期开展备份数据验证，一级数据每月验证一次，二级数据每季度验证一次，三级及以下数据每半年验证一次。验证内容包括数据完整性（哈希值比对）、可用性（模拟恢复测试）及加密有效性，验证失败需立即重新备份并分析原因，验证记录留存不少于 5 年。
5.2.2 制定“分级恢复预案”，明确不同级别数据的恢复优先级及目标：一级数据的恢复时间目标（RTO）不超过 2 小时，数据丢失目标（RPO）不超过 30 分钟；二级数据的 RTO 不超过 4 小时，RPO 不超过 2 小时；三级及以下数据的 RTO 不超过 12 小时，确保核心 EEG 数据的快速恢复。

5.2.3 每年至少开展一次全流程恢复演练，模拟存储设备故障、勒索病毒攻击等场景，重点测试一级、二级数据的恢复效率及应急预案的可行性。演练后形成复盘报告，针对问题优化备份策略及恢复流程，演练记录需提交伦理审查委员会备案。
5.2.3 定期组织数据恢复演练，每年至少开展一次全面的恢复演练，针对演练过程中发现的问题及时优化恢复预案及备份策略，确保在数据发生丢失或损坏时能够快速、有效地完成恢复工作。
6. 数据保存期限
6.1 通用保存期限
6.1 通用保存期限
结合学术研究规范、生物数据保护要求及教育数据特点，本数据集数据的通用保存期限规定如下：
6.1.1 一级数据（EEG 原始信号等）：永久保存，或按照国家生物数据管理相关规定及伦理审查意见确定保存期限；若学习者提出删除申请且符合伦理要求，可在完成学术成果追溯备案后进行销毁。
6.1.2 二级数据（预处理数据、知情同意书等）：保存期限不少于 15 年，自数据采集完成之日起计算，确保覆盖学术成果的生命周期及可能的追溯需求。
6.1.3 三级数据（去标识化学习者信息等）：保存期限不少于 8 年，自数据产生之日起计算，期满后经伦理审查委员会审核方可处理。
6.1.4 四级数据（公开元数据等）：可长期保存，若数据集停止服务，需提前 6 个月在学术平台公示，保障已引用用户的权益。
6.1.5 伦理审查文件、知情同意书：保存期限不短于数据本身保存期限，且至少保留 20 年，符合学术伦理追溯要求。
6.1.1 一级数据：永久保存，或按照国家相关保密规定及业务特殊要求确定保存期限；
6.1.2 二级数据：保存期限不少于 10 年，自数据产生之日起计算；
6.1.3 三级数据：保存期限不少于 5 年，自数据产生之日起计算；
6.1.4 四级数据：保存期限不少于 2 年，或根据业务需求及信息价值确定保存期限。
6.2 特殊保存期限
6.2.1 涉及学习者生物识别信息的数据，其保存期限需严格遵循《个人信息保护法》及伦理承诺，若学习者在保存期内书面申请撤回同意或删除数据，需立即启动审核流程：对于未用于已发表学术成果的数据，审核通过后 15 个工作日内完成销毁；对于已用于学术成果的数据，需向学习者说明情况并提供成果追溯证明，在征得同意后对原始数据进行匿名化处理（确保无法关联至个人）。
6.2.2 与学术论文、科研项目相关的数据，保存期限需满足科研项目验收（一般为项目结题后 10 年）及论文检索平台（如 CNKI、Web of Science）的追溯要求，若通用保存期限短于上述要求，以最长期限为准。
6.2.3 若数据集涉及重大科研成果（如国家级奖项、核心技术突破），一级、二级数据的保存期限需延长至 30 年，或按照相关主管部门要求执行。
6.2.4 未成年人学习者的数据，保存期限需至其成年后额外保留 5 年，确保符合未成年人权益保护要求。
6.2.1 涉及个人信息的数据，其保存期限需遵循《中华人民共和国个人信息保护法》等相关规定，不得超出实现处理目的所必要的最短期限。若法律、行政法规

另有规定的，从其规定。数据主体要求删除个人信息的，在核实身份及符合相关条件后，应及时删除或进行匿名化处理，不再保留。
6.2.2 涉及合同、协议、交易记录等与法律纠纷、审计监管相关的数据，其保存期限需满足诉讼时效、审计追溯等要求，若通用保存期限短于相关要求的，以相关要求为准。
6.2.3 学术研究数据的保存期限需符合学术规范及科研项目管理要求，原则上需保存至项目结题后至少 5 年，若涉及重大科研成果或有特殊要求的，需延长保存期限。
6.3 期限管理
建立数据保存期限台账，对各类数据的产生时间、保存期限、到期处理方式等信息进行记录。数据即将到期前 3 个月，由数据管理部门提醒相关业务部门对数据进行评估，确定是否需要延长保存期限或进行后续处理。对于无需延长保存期限的数据，按照规定的销毁流程进行处理。
7. 数据归档管理
7.1 归档范围
7.1 归档范围
符合以下条件的数据需进行归档处理，归档优先级依次为一级、二级数据：
7.1.1 完成数据预处理及标注后，超出日常分析周期但仍在保存期限内的 EEG 原始数据及衍生数据；
7.1.2 科研项目结题或学术论文发表后，需长期留存的核心研究数据及伦理支撑文件；
7.1.3 存储介质即将报废或系统升级前，需迁移保存的敏感数据；
7.1.4 伦理审查委员会要求归档的其他数据（如学习者投诉处理记录）。
7.1.1 超过日常使用周期，但仍在规定保存期限内的数据；
7.1.2 完成阶段性业务或科研项目后，需长期留存的数据；
7.1.3 按照法律法规及行业标准要求需归档保存的数据；
7.1.4 其他具有长期保存价值的数据。
7.2 归档流程
7.2 归档流程
7.2.1 数据归档需由项目负责人提出申请，填写《EEG 数据集归档申请表》，明确归档数据的类别、级别、数量、关联学术成果（如论文 DOI）及保存期限，经伦理审查委员会复核后，提交数据管理部门审批。
7.2.2 数据管理部门联合技术团队对归档数据进行“三重审核”：数据完整性（确保无缺失、无损坏）、合规性（去标识化处理符合要求）、安全性（加密状态有效），审核通过后进行归档预处理，包括数据格式标准化（如 EEG 数据转换为 EDF+通用格式）、关联信息标注（如实验编号、学习者分组）。
7.2.3 归档数据需存储于专用的学术归档系统（支持长期保存及学术检索），并为每批归档数据分配唯一的学术档案编号，建立“数据-成果-伦理文件”关联索引，便于后续检索与追溯。归档完成后需向项目负责人及伦理审查委员会提交归档确认报告。
7.2.2 数据管理部门对申请归档的数据进行审核，包括数据的完整性、准确性、合规性等，审核通过后，组织开展数据归档工作。归档前需对数据进行整理、清洗及加密处理，确保归档数据的质量和安全。

7.2.3 归档数据需存储在专用的归档存储系统中，归档存储系统需具备安全可靠、容量可扩展、访问便捷等特点。同时，为归档数据建立详细的档案目录，包括数据标识、归档时间、归档人员、存储位置等信息，便于检索和管理。
7.3 归档数据访问
7.3 归档数据访问
归档数据的访问严格限定于学术研究用途，需履行“学术资质+伦理承诺”双重审批流程：访问者需提交《归档数据访问申请表》，说明所在单位、研究方向、访问用途及数据使用伦理承诺，提供相关学术证明（如课题立项书、导师推荐信），经项目负责人、数据管理部门及伦理审查委员会三级审批同意后，方可获得授权。访问授权采用“权限最小化+时间限制”原则，一级数据仅开放数据使用权限（禁止下载原始文件），二级数据可授权有限下载权限，且下载数据需附加水印（含访问者信息）。访问过程全程日志记录，包括访问时间、操作内容、数据使用进展等，日志保存期限与归档数据一致。
8. 数据销毁管理
8.1 销毁条件
8.1 销毁条件
符合以下条件的数据，经严格审批后可进行销毁处理，一级、二级数据需额外经伦理审查委员会表决通过：
8.1.1 已达到规定保存期限，且经项目负责人、伦理审查委员会审核确认无学术追溯价值及继续保存必要的数据；
8.1.2 学习者提出合法删除申请，且数据未用于已发表学术成果，或已完成学术成果追溯备案的数据；
8.1.3 数据存在严重质量问题（如 EEG 信号受严重干扰无法修复），且无重新采集可能，经技术团队及项目负责人确认无保留价值的数据；
8.1.4 因政策调整或伦理要求，需强制销毁的敏感数据；
8.1.5 存储介质损坏无法修复，且无备份数据的残留数据（需对介质进行物理销毁）。
8.1.1 已达到规定的保存期限，且经评估无继续保存价值的数据；
8.1.2 数据存在严重错误或冗余，且无法修正或无保留必要的数据；
8.1.3 因业务调整、系统升级等原因，不再需要保留的数据；
8.1.4 法律法规及相关规定要求销毁的数据。
8.2 销毁流程
8.2 销毁流程
8.2.1 数据销毁需由项目负责人或数据管理部门提出申请，填写《EEG 数据集销毁申请表》，详细说明销毁数据的类别、级别、数量、关联学术成果状态、销毁原因及拟采用的销毁方式，附学习者删除申请（如适用）、数据质量评估报告等支撑材料，经部门负责人审核后，提交伦理审查委员会及数据安全管理委员会联合审批。
8.2.2 审批通过后，由数据管理部门、技术团队及伦理审查委员会代表组成销毁工作组，实施销毁操作并全程监督。销毁前需对数据进行最终备份校验（确保无重要数据遗漏），并断开所有访问权限。
8.2.3 销毁完成后，工作组需共同签署《数据销毁确认书》，明确销毁结果及责任，提交伦理审查委员会及数据安全管理委员会备案。

8.2.2 审批通过后，由数据管理部门组织实施数据销毁工作。销毁过程需指定专人负责监督，确保销毁操作符合规定流程。根据数据存储介质的不同，采用相应的销毁方式，确保数据无法被恢复。
8.3 销毁方式
8.3 销毁方式
8.3.1 电子数据销毁：针对一级、二级数据采用“多重销毁+介质处理”方式，先通过专业销毁软件（如 Blancco）对数据进行 7 次覆写，再进行消磁处理；对于存储过一级数据的硬盘、U 盘等介质，销毁后需进行物理粉碎（颗粒度不大于 2mm）或熔炼处理，确保数据彻底不可恢复。三级、四级数据可采用软件覆写或格式化+消磁方式销毁。
8.3.2 纸质数据销毁：包括知情同意书原件、伦理批件复印件等纸质材料，需采用专业碎纸机粉碎（保密等级不低于 4 级）或委托具备资质的第三方机构进行焚烧处理，销毁过程需拍照留存证据。
8.3.3 云存储数据销毁：需向云服务商出具书面销毁通知，要求其采用符合本政策的销毁方式，并提供销毁完成证明及数据不可恢复承诺，相关文件与销毁记录一并归档。
8.3.2 纸质数据销毁：对于纸质形式保存的数据及档案，采用粉碎、焚烧等方式进行销毁，确保纸质载体上的信息无法被读取。
8.4 销毁记录
8.4 销毁记录
数据销毁完成后，需建立“全流程销毁档案”，包括《销毁申请表》《审批意见》《销毁操作记录》《销毁确认书》、过程照片或视频、介质处理证明等，档案需以纸质+电子加密形式保存，保存期限不少于 10 年，以备学术伦理审查及监管部门核查。
9. 数据访问与使用控制
9.1 访问权限管理
9.1 访问权限管理
9.1.1 建立“学术身份+角色权限”双重控制机制，基于研究需求为用户分配权限：核心研究人员可访问一级、二级数据；合作研究人员需经项目负责人授权，仅可访问二级及以下数据；外部学术用户仅可申请访问三级、四级数据或经匿名化处理的一级数据片段。权限申请需提供单位推荐信及伦理承诺函。
9.1.2 对一级数据实行“双人操作+全程留痕”制度，数据查询、导出等操作需由两名授权人员分别验证身份（如指纹+动态密码），操作过程自动生成不可篡改的日志，日志内容包括操作人、操作时间、数据标识、操作结果等。
9.1.3 每半年开展一次权限审计，重点核查一级、二级数据的访问记录，清理闲置权限、超额权限，对异常访问行为（如非工作时间大量下载）启动调查程序，审计报告提交伦理审查委员会。
9.1.2 对于一级、二级敏感数据，实行“双人授权、双人操作”制度，重要操作需由两名及以上授权人员共同完成，确保数据操作的安全性和合规性。
9.1.3 定期对用户访问权限进行审计和清理，每年至少开展一次全面的权限审计工作，及时回收闲置、过期或超出职责范围的权限，避免权限滥用导致数据安全风险。
9.2 访问行为监控
9.2 访问行为监控

建立“实时监控+异常告警”系统，对数据访问行为进行全维度监控：针对一级数据的访问，实时监测登录 IP、操作频率、数据下载量等指标；针对二级数据，重点监控数据导出、复制行为。当系统检测到异常行为（如 IP 地址异常、超额下载、尝试破解加密）时，立即触发多级告警（技术负责人、项目负责人、伦理审查委员会），同时自动冻结相关访问权限，留存完整的行为日志用于调查。
9.3 数据使用规范
9.3 数据使用规范
用户在使用本数据集数据时，需严格遵守“学术用途唯一”原则，不得超出申请用途使用数据，不得将数据用于商业开发、非授权研究或其他违规场景；不得尝试对去标识化数据进行重新标识（如关联其他数据库追溯学习者身份）；不得擅自向第三方转让、共享数据，如需合作使用需重新提交审批。
使用一级、二级数据发表学术成果时，需在论文中注明数据集伦理审查编号及数据访问授权号，并引用本数据集的规范引用格式；成果发表后需将论文全文提交数据管理部门归档，作为数据追溯的依据。
对于违反使用规范的用户，立即终止其访问权限，收回已提供的数据，情节严重的通报其所在单位及学术期刊，同时保留追究其伦理及法律责任的权利。
10. 安全保障与责任追究
10.1 安全保障措施
10.1.1 技术保障：建立完善的数据库安全技术体系，包括数据加密、访问控制、入侵检测、防病毒、安全审计、数据脱敏等技术手段，定期对技术防护措施进行升级和优化，提升数据安全防护能力。
10.1.2 管理保障：建立健全数据安全管理组织架构，明确数据管理部门及各业务部门的安全职责，配备专职的数据安全管理人员，负责数据安全的日常管理、监督及应急处置工作。定期组织数据安全培训，提高全员的数据安全意识和操作技能。
10.1.3 应急保障：制定数据安全应急预案，明确应急组织机构、应急响应流程、应急处置措施及责任分工等内容。定期组织应急演练，提高应对数据安全事件的快速响应和处置能力。当发生数据安全事件时，需立即启动应急预案，采取有效措施控制事态发展，减少损失，并按照规定及时向相关部门报告。
10.2 责任追究
对于违反本政策规定的行为，如未经授权访问、使用、泄露、篡改、销毁数据，或未履行数据保存管理职责导致数据安全事件发生的，将根据情节轻重及造成的后果，对相关责任人进行处理，包括但不限于通报批评、经济处罚、岗位调整、纪律处分等；若行为触犯法律法规的，将依法追究其法律责任。外部合作单位及个人违反本政策规定的，将依据合作协议追究其违约责任，情节严重的，终止合作关系，并依法追究法律责任。
11. 附则
11.1 本政策由[数据管理部门名称]负责解释和修订，根据国家法律法规、监管要求及业务发展情况，可适时对本政策进行更新和完善，修订后的政策需提前向相关部门及人员公示。
11.2 本政策未尽事宜，参照国家相关法律法规、行业标准及本数据库其他相关管理制度执行。
11.3 本政策自发布之日起正式施行。
[北华大学]

［发布日期：2025 年 11 月］