ICS 93.020
CCS P 02

DB3205

苏 州 市 地 方 标 准

DB 3205/T XXXX—2025

智慧教育大平台通用规范

General specifications for smart education platform

（征求意见稿）

2025－XX－XX 发布　　2025－XX－XX 实施

苏州市市场监督管理局　　发 布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由苏州市电化教育馆提出。

本文件由苏州市市场监督管理局归口。

本文件起草单位：苏州市电化教育馆。

本文件主要起草人：

智慧教育大平台通用规范

1 范围

本文件规定了智慧教育大平台的平台建设要求、数据要求、功能要求、技术要求、运行管理、安全要求和监督管理。

本文件适用于苏州市范围内市级、市（县）区的智慧教育大平台的建设、服务支撑与运维管理。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 2260 中华人民共和国行政区划代码

GB/T 2261（所有部分） 个人基本信息分类与代码

GB/T 3304 中国各民族名称的罗马字母拼写法和代码

GB/T 4658 学历代码

GB/T 4761 家庭关系代码

GB/T 4762 政治面貌代码

GB/T 6864 中华人民共和国学位代码

GB/T 12407 职务级别代码

GB 18030 信息技术 中文编码字符集

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 25000.51 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

GB/T 29765 信息安全技术 数据备份与恢复产品技术要求与测试评价方法

GB/T 34998 移动终端浏览器软件技术要求

GA/T 2000.27 公安信息代码 第27部分：户口性质分类与代码

GM/T 0054 信息系统密码应用基本要求

JY/T 0644 数字教育资源基础分类代码

JY/T 1001 教育管理信息 教育管理基础代码

3 术语和定义

下列术语和定义适用于本文件。

3.1

智慧教育大平台 smart education platform

依托云计算、大数据、人工智能、物联网等新一代信息技术，整合各类教育资源，构建的一个集教学、管理、服务、评价等多种功能于一体的综合性数字化教育服务平台

3.2

区市一体 integration of districts and cities

在特定的区域范围内，将城区（或特定区域）与周边市（县、镇等）在经济、社会、行政、空间等多个方面进行有机整合、协同发展，打破传统的行政区划界限和体制机制障碍，实现资源共享、优势互补、共同发展，形成一个紧密联系、功能互补、协调统一的整体。

4 平台建设要求

4.1 基本要求

4.1.1 应遵循“政府引导、市场运作、产业发展、企业需要”的原则，充分调动社会力量参与，统筹规划建设服务平台。

4.1.2 应打造智慧教育之用户、数据、应用等三个基座，建成服务全市的智慧教育大平台基础框架，具备数据汇聚和应用融合能力。

4.1.3 应通过 Web 端、PC 端、phone 端、微信端等，或依托地方政府平台嵌入智慧教育大平台系统。

4.1.4 智慧教育大平台应建立健全管理体系，制定相应的工作、技术、管理制度。

4.1.5 智慧教育大平台应规范服务流程，编制服务指南，并在平台公布。

4.1.6 智慧教育大平台应引进专业服务机构、专家入驻平台，并开展服务事项完成率、及时性、满意度等动态评价，实行动态管理。

4.2 平台框架

智慧教育大平台建设整体架构见图1。

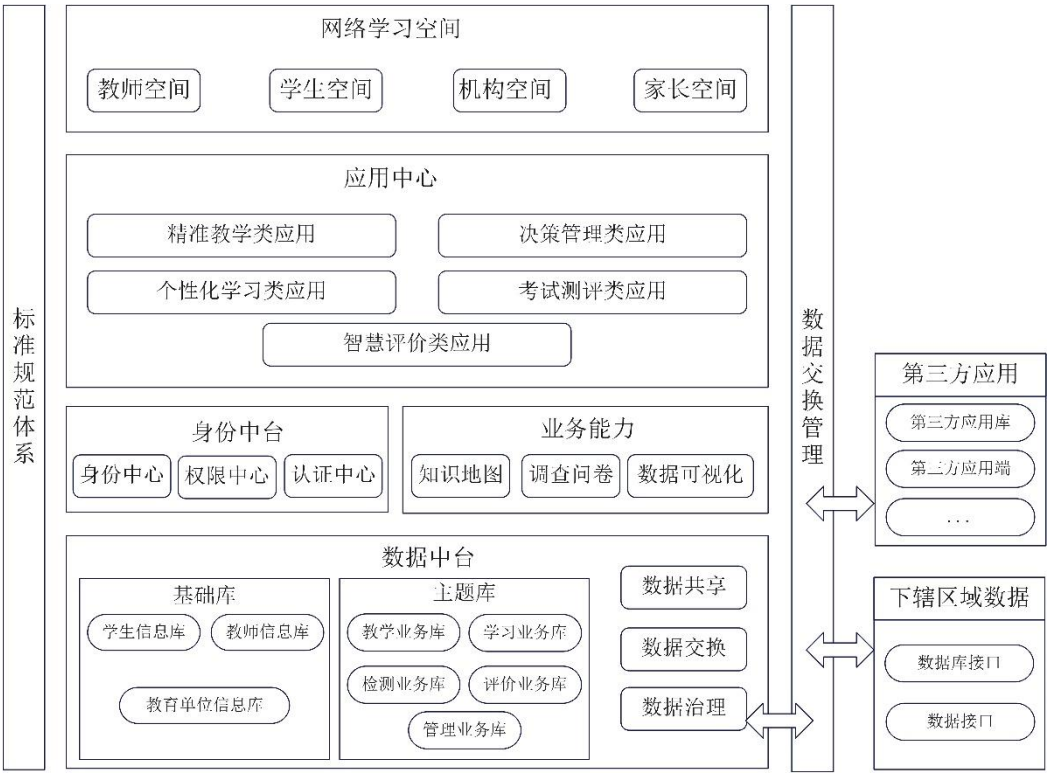

图1 整体架构

4.3 身份中台

4.3.1 应构建“区市一体”的可支撑有机运行、灵活适配的大平台用户基座，建设内容包括但不限于：

a) 身份中台涵盖教育体系内/外多角色、身份、职位的用户体系；
b) 支撑多级管理的组织架构与运行维护体系；
c) 支持用户角色、权限与应用可配置的认证体系；
d) 支持多模式的单点登录。

4.3.2 应建立底层统一的用户、角色、用户角色、角色权限数据表，实行分级分层管理与维护机制。

4.3.3 建立集中统一认证机制，实现用户登录认证后即可获得相应功能模块（子系统）使用操作权限。

4.3.4 实现组织机构、用户角色权限的自定义和灵活配置，自主构建多级组织机构，设置用户角色，分配用户权限。

4.3.5 采用市、区、学校多级管理模式，上级管理员可以设置、定义和管理下一级管理员，本级管理员可以设置和定义本级组织机构、业务管理人员及用户。

4.3.6 身份中台管理包含身份中心、权限中心和认证中心，内容如下：

a) 身份中心：包含用户管理、角色管理、组织机构管理、学校管理、教师管理和学生管理等；
b) 权限中心：设置应用权限，指定应用服务公开权限和设置各应用模块的负责人；
c) 认证中心：建立统一的身份配给和身份认证体系，实现角色、权限的动态同步，实现多种登录认证方式，实现“一次登录，处处适用”。

4.4 网络学习空间

4.4.1 网络学习空间包括个人和机构两大用户，个人用户包括学生、教师、家长等。机构空间需涵盖教育系统各级各类职能部门和相关管理部门。

4.4.2 用户应用空间界面与交互设计，实现涵盖多角色、多身份的定向应用集成与数据推送，支持多角色、多身份用户空间的功能切换与应用对接。

4.4.3 应打造师生全生命周期和全业务流程管理平台，实现教学与教育管理、家校互动、教育信息发布与反馈等各类应用服务的无缝对接。

4.4.4 应建设支撑各类用户应用需要的功能组件与功能配置，如消息推送、信息维护、创建群组、机构数据管理、活动管理、文件审批、通知公告、问卷系统研发等；组建数据可视化应用服务、知识地图系统。

4.4.5 打造“区市一体”的智慧教育协同创新体系，实现线上机构与线下机构教育管理的融合对接，建设机构数据中心。

4.5 数据中台

4.5.1 应对接学生、教师基础数据，实现“一数一源”，建立统一的数据资源资产规范，包括数据清单、系统清单、对政务云需求清单等。

4.5.2 应编撰苏州基础教育数据标准规范体系，统筹全市教育数据采集、汇聚、管理、分析与应用等五个环节，构建数据围绕的区域教育生态系统。

4.5.3 应做到全量数据服务的四大能力，内容包括：

a) 数据聚合能力：数据采集、清洗、转换、聚合、装载等能力；
b) 数据整合能力：各级各类学校采用的主流应用系统和线下数据的整合能力，对于用户必需的其他来源数据；
c) 数据治理能力：数据结构、数据属性、数据接口、数据质量的管理能力，以及对非结构化日志及物联网数据的管理能力；
d) 数据共享能力：以应用的视角对全量数据资源进行有效运用。

4.6 应用中心

为用户提供义务教育优质均衡发展监测系统、课后服务管理系统、数字化体育卫生系统等功能，与教育局系统进行连接，实现信息共享和业务协同，为学校、机构、教师、学生提供服务。

4.7 平台体系

4.7.1 应建立统一的数据标准、技术规范，指导平台开发建设和运营管理的全过程。

4.7.2 应按照国家相关安全等级保护的要求进行安全保障体系的建设，确保系统运行过程中的物理安全、网络安全、数据安全、应用安全、访问安全等。

5 数据要求

5.1 基本要求

5.1.1 数据代码应符合 GB/T 2260、GB/T 2261（所有部分）、GB/T 3304、GB/T 4658、GB/T 6864、GB/T 4761、GB/T 4762、GB/T 12407、JY/T 0644、JY/T 1001、GA/T 2000.27 等要求。

5.1.2 教育基础数据应划分为以下 4 个基础数据子集：

——学生基础数据子集：学生管理基础数据元素的集合；

——教师基础数据子集：教师管理基础数据元素的集合；

——学校基础数据子集：学校概况基础数据元素的集合；

——机构基础数据子集：机构概况基础数据元素的集合。

5.1.3 数据元素组成应通过数据项进行描述和规范，元数据结构如下：

a) 编号：数据元素的唯一标识；

b) 数据项名：由“中文简称”每个汉字的拼音首字母（大写）组成，且与其一一对应，宜在实际数据结构中采用；

c) 中文名称：数据元素的中文指称；

d) 约束：数据元素约束状态的描述，字母“M”表示“必备”数据元素、字母“O”表示“可选”数据元素；

e) 数据类型：数据元素的数据类型要求；

f) 数据格式：数据元素的格式要求；

g) 值域：数据元素的允许值集合；

h) 说明：数据元素的解释、举例。

5.1.4 数据类型和可能的取值见表 1。

表1 数据类型和取值

数据类型	表示	说明
字符型（string）	C	以字符表达的数据元值的类型，可用于表达字母、数字、汉字和其他字符形式，采用GB 18030中规定的字符
数值型（numeric）	N	以任意实数表达的数据元值的类型
日期型（date）	D	以日期表达的数据元值的类型，形式符合GB/T 7408的规定
二进制类（binary）	B	以二进制编码表达的数据元值的类型
集合（set）	S	用于存放其他数据的容器，集合中可嵌套其他集合

5.1.5 数据格式应从业务角度规定数据元素值格式需求，包括所允许的最大或（和）最小字符长度、

数据元素值的表示格式等。数据格式中使用的字符含义如下：

a) 字母“a”表示字符；
b) 字母“n”表示数值；
c) 字母“a”或“n”之后的自然数表示定长个字符（字符集默认为GB 18030），或数值的十进制最大位数；
d) 字符串“.ul”表示长度不确定；
e) 逗号“，”隔开的两个自然数“p,q”表示数值最大p个十进制位数，小数点后q位；
f) 双点号“..”表示从最小长度到最大长度，前面附加最小长度，后面附加最大长度；
g) 字符串“YYYYMMDD”中的“YYYY”表示年份，“MM”表示月份，“DD”表示日期，可以视实际情况组合使用。

5.1.6 应根据相应属性，规定数据类型、长度来决定数据元素的允许值集合。值域可不作要求或通过以下方式给出：

a) 通过参考和引用相关标准；
b) 通过文字描述给出值域的限制；
c) 通过列举方式给出所有可能的取值，以及每一个值对应的实例或含义；
d) 通过规则间接给出；
e) 无要求。

5.2 学生基础数据

5.2.1 学生基础数据包含学生基础数据和扩展信息数据，具体内容如下：

a) 学生基础数据：学生基本信息数据；
b) 学生扩展信息数据：家庭成员基本信息数据、监护人信息数据、幼儿园学籍信息数据、小学学籍信息数据、初中学籍信息数据、高中学籍信息数据、现就读信息数据子类、学生履历信息数据。

5.2.2 通过数据掌握学生的真实现状和学生基础数据，为开发利用与变化状况提供数据基础。

5.3 教师基础数据

5.3.1 教师基础数据包含教师基础数据和扩展信息数据，具体内容如下：

a) 教师基础数据：教师基本信息数据；
b) 教师扩展信息数据：教师任教信息数据、教师在校学习经历数据、教师工作经历数据。

5.3.2 可为学校、机构提供管控数据依据。

5.4 学校基础数据

5.4.1 学校基础数据包含学校基本信息数据和扩展信息数据，具体内容如下：

a) 学校基础数据：学校基本信息数据；
b) 学校扩展信息数据：学校班级信息数据、学校校区信息数据。

5.4.2 帮助学校管理者提供数据基础。

5.5 机构基础数据

5.5.1 机构基础数据包含机构基础数据、扩展信息数据和其他机构信息数据，具体内容如下：

a) 机构基础数据：教育行政部门信息数据、教育直属事业单位信息数据；
b) 机构扩展信息数据：教育行政部门处室信息数据；
c) 其他机构信息数据：人员体检机构信息数据、校外培训机构信息数据。

5.5.2　整合各项与学生、教师有关的机构，为智慧教育大平台提供数据支撑。

6　系统功能要求

6.1　精准教学类应用

6.1.1　基本要求

6.1.1.1　应基于数据积累和融合，兼顾个体和群体的大量动态数据库，利用教育大数据等技术分析，及时了解学生学习状况和教师教学情况。

6.1.1.2　对学生成绩和学习效果进行预测，实施精准教学完成个性化学习服务。应用场景包括：课堂教学、智能教辅系统、在线教学平台、计算机自适应考试系统、特殊教育服务平台等。

6.1.2　课堂教学

6.1.2.1　应通过多阶段动态的教育表征模型，对教学过程以及教育场景进行分析和优化，对学习主体和学习策略的交互作用进行动态建模。

6.1.2.2　应将精准教学理念带入传统课堂，利用云计算、大数据、人工智能等信息技术，打造课前（大数据学情诊断）、课中（人工智能教室）、课后（AI 学习系统）的教学闭环场景，内容包括但不限于：

a)　课前引导学生预习并进行学前测试、根据学情分析重构学案设计；
b)　课中实施分层分组的教学互动，综合历史数据和课堂表现进行差异化指导；
c)　课后针对性推送分层作业，有效实施教学干预，并布置下一个周期个性化自主学习任务。

6.1.3　智能教辅系统

6.1.3.1　应构建教育产生的海量数据后台为基础，提供学生认知诊断平台，进行课程资源的精准供给和学习服务的精准定制。

6.1.3.2　利用大数据实现规模化教育下的个性化教育，围绕“因材施教”提供覆盖教、学、考、评、管的教育全场景解决方案。

6.1.4　在线教育平台

在线教育平台应以物联感知技术为基础，开展实时数据采集，记录学习时长，根据平时作业、学习时长、讨论合作综合评判平时成绩，提高课程推荐系统的精准度，实现针对学生个体和教学过程的全过程精准教学模式。

6.1.5　计算机自适应考试系统

6.1.5.1　应根据学生在平台内完成测试的情况，及时更新下一道题目的难易程度，达到千人千卷、精细测量的效果。

6.1.5.2　根据历史答题数据及时调整题库内容，精确题目参数、优化推荐精度，满足准确的个性化需求。

6.1.6　特殊教育服务平台

6.1.6.1　应以信息化、智能化技术手段，发展沉浸式学习资源创建技术，制作符合特殊群体认知特点的交互式学习资源。

6.1.6.2　应以全程测量数据为依据，完成技能达成项目教学。

6.2 决策管理类应用

6.2.1 总体要求

6.2.1.1 决策管理类应用根据不同层面应具备不同管理系统，具体内容如下：

a) 学校层面：教务管理系统、办公系统等；
b) 教育局层面：教育均衡发展检测系统、校外培训机构管理平台等。

6.2.2 学校层面

6.2.2.1 教务管理系统通过集成各种功能提高教务工作的效率和质量，包含以下几个核心功能：

a) 教师管理系统：允许教务人员添加、修改、删除和查询教师信息；
b) 班级信息管理：包含班级信息的添加、修改、删除和查询；
c) 学生信息管理：设计学生信息的维护；
d) 课程信息管理：管理课程基本信息，包括添加、修改、删除和班级课程设置；
e) 成绩信息管理：及时汇总学生成绩并出具报告；
f) 财务信息管理：设计学生缴费、欠费管理和查询；
g) 打印信息管理：允许打印学生成绩、选课表和班级表等。

6.2.2.2 办公系统通过集成多种功能来提高学校行政和教学管理的效率，包含以下功能：

a) 智慧考勤：包括上下班登记、外出登记、请假登记、出差登记等，能够生成考勤报表，实现统计汇总和分析；
b) 校园通讯录：包括通讯录、个人通讯录和公共通讯录，支持通讯录人员的导入导出操作；
c) 日程计划：包括我的工作日程，可以方便用户查询当日员工外出情况；
d) 流程审批：支持退文功能，可以退到以前的任何一级，也可以退回到发起人。审批过程中支持痕迹保留，电子印章，手写签名、全文批注；
e) 数据管理：包括数据基础管理、数据资源管理、数据服务应用等；
f) 应用支撑服务平台：提供基础信息管理、接入规范管理、开放应用中心、统一认证平台等功能；
g) 教学考评管理应用：包括智慧教学、智慧学习、智慧考试、智慧评价、智慧管理等；
h) 云平台设施：涉及数据机房、云平台建设、网络设施等；
i) 网络设施：包括校园网络系统、IP 广播系统、综合布线系统等；
j) 安全与隐私保护：包括用户身份验证、数据加密、操作记录等，确保数据安全，避免信息泄露。

6.2.3 教育局层面

6.2.3.1 运用教育均衡发展检测系统，实现县域义务教育优质均衡发展年度监测数据的采集，并按指标要求进行数据的统计、计算与处理，并自动生成相关统计报表，包含以下功能：

a) 义务教育优质均衡评估：提取义务教育优质均衡发展相关数据进行数据的统计、计算与处理，形成评估结论，生成评估报告、达标比例及达标建议；
b) 义务教育优质均衡年度监测：实现市级管理职能机构（部门）启动年度监测工作，将上报的数据按年度监测指标要求进行统计、计算与处理，诊断达标情况，生成监测报告、达标比例以及达标建议。

6.2.3.2 应搭建“部门监管服务、机构合规运营、学生家长放心”的校外培训机构管理平台，功能如下：

a) 智能搜索功能：快速找到附近合法的校外培训机构，同时提供校外培训机构的详细信息和评价，方便家长和学生选择适合自己的机构；

b） 在线评估服务：家长和学生可以通过平台提供的在线测试来评估自己的学习水平和能力，根据评估结果来选择适合自己的课程和培训机构；
c） 在线预约服务：通过平台预约校外培训机构的课程；
d） 安全监管服务：对校外培训机构进行监管，确保机构的资质和证书合法有效和学生的人身安全和财务安全；
e） 在线学习资料和辅导服务：提供免费的在线学习资料和辅导服务。

6.3 个性化学习类应用

智慧教育个性化学习类应用通常具备以下功能：
a） 个性化学习计划：根据学生的学习能力、兴趣和学习历史，自动生成个性化的学习计划；
b） 智能推荐：利用算法推荐适合学生水平和兴趣的课程、教材和活动，针对薄弱环节，推送适配学习内容，调动学习积极性；
c） 学习进度跟踪：实时跟踪学生的学习进度，并提供可视化的学习路径；
d） 互动式学习：提供视频教学、卡通互动、即时学习评价等，丰富教学多样性、趣味性，提高学习兴趣；
e） 自适应学习：根据学生的表现自动调整学习内容的难度和深度，发挥学生学习主动性，落实学生在学习中的主体地位，让学生不再被动地跟随老师学习；
f） 在线评估与测试：提供在线测试和评估工具，帮助学生检验学习成果；
g） 反馈与指导：根据学生的学习表现提供即时反馈和个性化指导。

6.4 考试测评类应用

考试测评类应用应具备以下功能：
a） 题库管理：系统应包含一个全面的题库管理功能，允许管理员添加、编辑、删除题目，并支持多种题型，如单选题、多选题、判断题、填空题、问答题等；
b） 试卷生成：系统能够根据预设的规则或手动选择来生成试卷，支持随机组卷和固定组卷，以及多种组卷策略；
c） 在线考试：支持考生通过互联网进行在线考试，不受时间和地点的限制；
d） 考试监控：系统应提供考试监控功能，包括切屏限制、长时间不操作强制交卷等防作弊技术，确保考试的公平性；
e） 智能阅卷：客观题应支持自动评分，主观题可以提供关键词或模板匹配辅助阅卷；
f） 成绩统计与分析：系统应自动统计考生成绩，并提供数据分析和可视化报告，帮助组织者了解考生的表现和能力。

6.5 智慧评价类应用

智慧教育智慧评价类应用通过现代信息技术提升教育评价的科学性、专业性和客观性。具体功能如下：
a） 数据驱动的评价：利用大数据技术，全方位、全过程采集教学数据，包括情感因素、心理倾向、实践能力等非结构化数据；
b） 实时反馈与干预：通过跟踪和记录学生的学习过程，适时发起学习干预，为教师和学生提供动态、实时的评价反馈；
c） 学情分析与预警：基于数据分析，监测学生可能存在的学业风险，为这些学生提供个性化的帮助；

d) 自适应学习支持：提供基于大数据的自适应学习，动态匹配符合学生“最近发展区”的学习服务；
e) 多维度评价：关注学生的学业成绩，还包括品德、体育、美育、劳动教育等多个方面的综合评价；
f) 智能化评价工具：创新评价工具，利用人工智能、大数据等现代信息技术，探索开展学生各年级学习情况全过程纵向评价、德智体美劳全要素横向评价；
g) 个性化评价方案：为每个学生提供精细的“数字画像”，根据学生的知识结构、能力表现和内在潜能提供个性化的评价方案。

7 技术要求

7.1 基本要求

7.1.1 智慧教育大平台应实现并兼容 iOS、Android、Windows 等操作系统，数据接口基于标准的互联网协议，便于兼容与其他系统的数据交换。
7.1.2 服务器与数据库应支持系统的高并发等技术要求，配有相关的服务软件，支持移动应用，并应符合 GB/T 34998 的规定，系统软件还应满足 GB/T 25000.51 中的功能性、可靠性、易用性、维护性、可移植性的要求，并有容错和系统恢复能力。
7.1.3 操作系统、数据及中间件、应用层软件宜具有一定的容错能力。
7.1.4 智慧教育大平台应具有重要数据的备份方案，数据备份应符合 GB/T 29765 的相关规定。
7.1.5 系统密码应用应符合 GM/T 0054 的要求。

7.2 接口

7.2.1 系统应建立与其他管理系统（如有）的信息接入机制，宜使用开放标准的、可扩展的方式进行采集或接收。
7.2.2 系统与其他管理系统（如有）的接口集成文档应明确下列内容：
a) 接口目的；
b) 接口功能；
c) 接口物理特性；
d) 通信协议；
e) 接口测试；
f) 接口各方职责；
g) 接口点表。
7.2.3 接口信息传输速率应满足系统功能要求。

7.3 软件系统

7.3.1 操作系统和数据库系统的选择应符合下列要求：
a) 根据服务器配置要求以及应用软件需求，选择稳定可靠、多用户、多任务、性能优良、被广泛采用、符合安全要求的操作系统；
b) 根据数据应用规模，选择适用的并具备可扩展性、安全性、稳定性的数据库系统软件。
7.3.2 应用软件的设计应满足下列要求：
a) 根据系统的规模、用户数量、性能要求等，确定计算机设备选型和设备的配置方案；
b) 根据系统的功能要求，进行应用软件功能模块的划分，进行逻辑结构和数据流程设计；

c） 根据系统规模设计响应速度及并发性的性能需求，并留有一定余量，在系统规模不发生数量级变化的情况下，不出现明显的性能下降；留有升级接口和升级空间；
d） 进行安全性设计，不出现由于应用软件运行不安全而导致的系统安全性事故。

7.4 调试和验收

7.4.1 应在系统安装完成后进行调试。
7.4.2 调试前应具备下列条件：
a） 系统软件已按设计要求安装完毕；
b） 已制定调试和试运行方案；
c） 根据使用说明书校验功能的正常工作及数据准确性。
7.4.3 系统连续、安全、稳定试运行 1 个月后，组织竣工验收。验收不合格的应限期整改，整改完毕后进行试运行、复验；复验不合格，应再次整改并试运行、复验，直至验收合格。

8 运行管理

8.1 网络运行

8.1.1 管理单位应对正常运行中的系统进行在线监测，当出现数据中断或有差异时立即处理。
8.1.2 系统出现故障信号时，维护人员应迅速查明原因，修复故障。

8.2 运行环境

8.2.1 应使用正版、稳定的服务器操作系统，支持国产化应用，定期升级系统补丁，加强对密码的分级管理措施。
8.2.2 应使用主流应用服务器软件，要求应用服务器软件承载量高、安全性高、稳定性好。
8.2.3 应安装正版高性能杀毒软件，制定安全措施，定期升级病毒库，防止病毒感染。

8.3 身份鉴别

8.3.1 应提供专用的登录控制模块对登录用户进行身份标识和鉴别。
8.3.2 应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别。
8.3.3 应提供登录失败处理功能，可采取限制非法登录次数、自动退出等措施。

8.4 访问控制

8.4.1 基本要求

8.4.1.1 应由授权主体配置访问控制策略，并限制默认账户的访问权限。
8.4.1.2 应授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约关系。

8.4.2 用户注册安全

智慧教育大平台用户非面向大众用户，用户注册时应采用自上而下的授权的自动注册手段避免非法用户注册登录。即平台用户由对应的管理员进行维护，并进行相关授权。

8.4.3 用户认证鉴权

平台在用户登录时，应采取图片验证码和密码，错误达到上限后采取锁定账户等必要防护手段组织非法用户暴力破解账号；其次，可采用密码强制定期修改功能等必要手段，避免用户密码泄露带来的风险。

8.4.4 密码安全管理

用户在注册平台过程中，用户密码应避免弱密码原则。用户密码8位以上，密码中应包含数字、大写字母、小写字母、特殊字符等，且应避免明文存储，包括但不限于使用MD5加密等手段。

8.4.5 用户权限体系

平台应具备角色、用户二级以上的用户体系，保证组织架构分级管理。针对不同角色，提供不同的平台功能权限、资源使用权限和数据访问权限。

9 安全要求

9.1 数据

9.1.1 基本原则

9.1.1.1 职责明确

应按照数据安全管理不同角色的职责分工，明确其安全责任主体，按照“谁管理、谁负责”和“谁使用、谁负责”的原则，厘清数据流转中各方权利义务和法律责任。

9.1.1.2 最小授权

应根据数据需求，实现数据最小化访问，控制风险。保证只收集和处理满足目的所需的最少数据，从而减少数据安全风险，同时兼顾授权效率与体验。

9.1.1.3 责任不随数据转移

控制数据的组织应对数据负责，当数据转移给其他组织时，责任不随数据转移而转移。组织应完成以下流程：

a) 对数据转移给其他组织所造成的数据安全事件承担安全责任；在数据转移前进行风险评估，确保数据转移后的风险可承受；
b) 通过合同或其他有效措施，明确界定接收方接收的数据范围和要求，确保其提供同等或更高的数据保护水平，并明确接收方的数据安全责任；
c) 采取有效措施，确保数据转移后的安全事件责任可追溯。

9.1.1.4 安全

应采取适当的管理和技术措施，包括对数据分级，制定安全保障措施，确保数据安全。

9.1.1.5 可审计

实现对数据平台和数据应用各环节的数据审计，保证数据记录的完整性和操作可追溯。

9.1.2 基本框架

智慧教育大平台数据安全框架应依据“网络安全等级保护定级”“个人信息安全规范”和“信息安全事件分类分级”为安全准则指导，从人员访问、数据分级、数据生命周期安全管理、数据访问控制和数据安全审计5个方面进行规范，数据安全框架见图2。

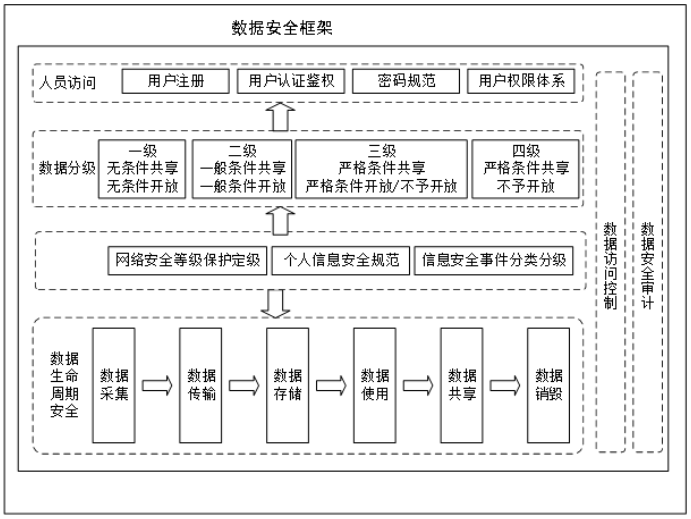

图2　数据安全框架

9.1.3　数据分级

9.1.3.1　教育数据宜采用“依法依规、自主定级、就高从严”的原则，由教育部门对数据进行分级。

9.1.3.2　教育数据分级应充分考虑教育数据的敏感程度，教育数据在发生数据泄露、非授权使用等安全事件后对党政机关、企事业单位和社会组织、自然人合法权益的危害程度确定教育数据的级别。

9.1.3.3　数据分级判定标准可分为一级、二级、三级和四级，具体数据分级见表 2。

表2　数据分级判定

数据级别	敏感程度	影响程度	共享属性	开放属性
一级	不敏感数据	数据在被篡改、破坏、泄露或非法获取、非法利用后无影响。	无条件共享	无条件开放
二级	低敏感数据	数据在被篡改、破坏、泄露或非法获取、非法利用后造成轻微影响。	一般条件共享	一般条件开放
三级	敏感数据	数据在被篡改、破坏、泄露或非法获取、非法利用造成一般影响。	严格条件共享	严格条件开放/不予开放
四级	高敏感数据	数据在被篡改、破坏、泄露或非法获取、非法利用后造成严重影响。	严格条件共享	不予开放

9.1.4　数据访问控制

平台对数据访问安全控制应提供必要功能。平台具备但不限于以下数据安全管控功能：

a)　平台支持最小授权原则分配用户权限，授予不同账户完成其工作内容所需的最小权限，并保留授权记录；

b)　平台根据数据分级规则，细粒度地控制用户访问数据；

c)　平台使用过程中，严格限制批量修改、拷贝、下载等操作的权限。

9.1.5　数据安全审计

智慧教育大平台的数据安全审计内容包含但不限于：

a) 平台开启操作系统日志、数据库日志、网络日志和应用日志，保存相关日志数据不少于 6 个月；
b) 平台审计覆盖到每个用户，对所有用户的各类数据访问和操作行为进行审计；
c) 平台审计记录包含足够的内容满足审计的需要，包括但不限于事件日期、时间、发起者信息、类型、描述和结果；
d) 平台审计记录保障完整性，只有授权人员有权限查看。不应以任何方式修改记录内容和未经许可删除记录；
e) 平台审计记录对内容敏感的字段应采用脱敏（关键信息用*代替）方式落地。敏感字段包括但不限于姓名、身份证号、用户、密码、密钥等；
f) 平台在信息处理设备、系统和主机采取措施保证系统的时钟同步，以保证审计记录的可追溯性和准确性。

9.1.6 数据生命周期安全管理

9.1.6.1 数据采集安全

智慧教育大平台采集数据时，包含以下内容：

a) 遵循合法、合规、必要、适度原则，按照法定范围采集数据；
b) 明确采集数据的方式、范围、数量、频率、目的和生命周期，确保最小范围内采集数据；
c) 提供相应数据采集清单，获取相关组织授权同意。第三方平台在提供学生、老师等个人敏感数据应额外加密，确保数据采集安全；
d) 平台记录数据采集的过程，支持数据采集操作可追溯；
e) 授权在职在编员工，办理数据采集的相关业务，并签订授权书，在符合保密协议的条件下按照要求承担相关工作，并接受委托单位的监督。
f) 提供共享库方式进行库表采集数据，遵循“一数据库实例一系统”原则，授权对应的数据库用户密码权限，确保最小授权原则，数据密码避免弱密码。

9.1.6.2 数据传输安全

智慧教育大平台传输数据时，应满足下列要求：

a) 建立加密传输手段，包括但不限于对称加密；
b) 应跟踪和记录数据传输过程，具备数据传输过程的可追溯能力；
c) 应保证传输过程中数据的保密性和完整性，记录传输的数据大小，时间等；
d) 应对敏感字段进行加密传输。敏感字段包括但不限于姓名、学籍号、身份证号码、手机号等；
e) 采集时使用安全的物理介质（如加密存储）进行数据传输，包括但不限于内部网络等；
f) 平台跨网络进行数据采集，在进行防火墙配置时，需要明确访问或者被访问的 IP 和端口，确保最小范围开通 IP 白名单。

9.1.6.3 数据存储安全

数据存储应满足以下要求：

a) 具备数据分片和分布式存储安全能力，满足分布式存储下分片数据完整性、一致性和保密性保护要求；
b) 具备数据逻辑存储隔离授权与操作，确保具备多租户数据存储安全隔离能力；

c） 数据加密存储应避免明文存储，通过对称加密等手段对字段进行加密落地。敏感字段包括但不限于姓名、身份证号码、手机号码等；
d） 数据备份与恢复应建立备份、归档、销毁、恢复机制，明确数据备份及归档的范围、频率、数据保存时长，明确数据恢复应急响应准入条件和工具，同时应具备对过期的归档数据进行及时彻底删除的能力。

9.1.6.4 数据使用安全

数据使用安全应满足以下要求：
a） 平台数据使用和分析处理的目的和范围，应符合网络安全法等国家相关法律法规要求；
b） 平台依据数据分级建立细粒度的数据访问控制机制，限定用户可访问数据范围；
c） 平台应具备完整的数据使用操作记录和管理能力；
d） 平台用户在治理数据时，确保所有输入数据都经过适当的验证和清洗；
e） 平台用户在加工数据时，定期备份数据，并确保可以在出现问题时迅速恢复数据。

9.1.6.5 数据共享安全

数据共享安全应具备以下要求：
a） 第三方平台申请共享时，应具备以下要求：
1） 遵循合法、合规、必要、适度原则，按照法定范围申请共享数据；
2） 明确申请共享数据的方式、范围、数量、频率、目的和生命周期，确保最小范围内申请共享数据。
b） 智慧教育大平台接受申请时，应具备以下要求：
1） 建立安全规范的第三方系统数据对接流程和数据保密协议；
2） 对第三方数据共享申请，需要经过严格审核，确保数据最小化共享。
a） 第三方平台申请数据共享时，应具备以下要求：
1） 明确数据共享的形式和标准，确保数据的可读性、可访问性、可重用性和安全性；
2） 按照“一系统一秘钥”的原则将敏感数据进行加密共享。敏感字段包括但不限于姓名、学校、年级、班级、身份证号码、用户密码等；
3） 具备时效性，在数据共享申请时效到期后，智慧教育大平台应自动收回数据共享权限。同时，应具备审计功能并定期审计，包含但不限于日志审计；
4） 在第三方平台进行数据共享时宜对第三方平台进行校验，包含但不限于 APPKEY 校验等。

9.1.6.6 数据销毁安全

平台应根据不同场景建立对应的数据删除机制，包括不限于下线系统中数据、前置采集服务器数据以及临时存放外发数据等场景。数据销毁前应进行确认，避免发生误操作导致数据丢失。

9.2 应用

9.2.1 应对用户访问网络资源的权限应有认证和控制。
9.2.2 系统管理人员应监督数据库使用权限、用户密码使用情况，用户应定期更换密码。

9.3 网络

9.3.1 智慧教育大平台网络应符合 GB/T 22239—2019 的第二级安全要求。
9.3.2 智慧教育大平台管理人员应对网络进行实时异常流量监控，定期对网络系统进行查询、检测，及时对故障进行隔离、排除和恢复。

9.3.3　智慧教育大平台应采用通信协议隔离技术和有攻击防御与溯源安全措施，保障信息传输的安全。

9.4　终端

9.4.1　应由专业技术人员负责系统软件、设备、设施的安装、调试、排除故障，其他单位和个人不应自行拆卸或安装任何软、硬件设施。

9.4.2　系统终端应设置防火墙，安装防病毒软件。

10　监督管理

10.1　智慧教育大平台监督方式主要包括内部监督、服务对象监督和行政主管部门监督。

10.2　智慧教育大平台应对自身进行内部监督。建立健全内部监督机制，定期对自身服务质量进行评价，对服务过程、服务结果的质量与问题等情况进行总结，对接受投诉情况及时反馈并改善。

10.3　智慧教育大平台应主动接受服务对象监督，并提供电话、网络和信件投诉等渠道，公开监督电话、邮箱、信箱等。

10.4　行政主管部门应对智慧教育大平台进行监督：

a)　不定期对智慧教育大平台的建设运营、投诉处置等情况进行调查监督；

b)　定期组织专家对智慧教育平台进行考核评价，督促智慧教育大平台持续改进。