

# DB4403

深圳市地方标准

DB4403/T XXX—XXXX

## 基础教育数字化转型建设规范 第2部分：数据共享交换

Specifications for the digital transformation of basic education  
—Part 2: Data sharing and exchange

(送审稿)

XXXX-XX-XX 发布

XXXX-XX-XX 实施

深圳市市场监督管理局 发布



目 次

前言 ..... II

引言 ..... III

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 数据共享交换规则 ..... 2

5 数据质量要求 ..... 2

6 数据服务要求 ..... 3

7 数据安全要求 ..... 3

8 数据伦理和隐私 ..... 4

参考文献 ..... 6

# 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。

DB4403/T XX—XXXX《基础教育数字化转型建设规范》分为以下3个部分：

- 第1部分：学校数字基座建设；
- 第2部分：数据共享交换；
- 第3部分：应用场景开发。

本文件是DB4403/T XX—XXXX的第2部分。

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这些专利的责任。

本部分由深圳市教育局提出并归口。

本文件起草单位：深圳市教育信息技术中心

本文件主要起草人：张惠敏、梁为、冯亮、李淼云、林雪芳、王凯利、戴俊雄、罗晓峰、何琼、盛晓澜、胡春风、纪显俐、阳小、金源、唐计、王杏璇、陈南兴、许婷婷、何泽洲。

# 引 言

党的二十大报告提出要大力推进国家教育数字化战略行动。深圳市委2023年部署的重要任务中也提出要推进教育数字化，建设全民终身学习的学习型社会、学习型城市。规范建设，标准先行。要在全市大力推动教育数字化转型，就要先建立一套适合全市中小学校数字化转型发展的标准规范。开展《基础教育数字化转型建设规范》编制，有助于推进全市整体规划统筹，整区推进、以学校为最小建设单位，推动“政府定标准、搭平台，企业做产品、保运维，学校购买服务、建资源”的数字化建设及运维模式，促进教育管理业务重组和流程优化，支持管理决策和教育治理，促进校区市三级数据的有效融通共享，为普通中小学校进行技术减负、管理减负，推进教育数字化转型来赋能教育变革和高质量发展。同时，这对于从整体监测和评价深圳市普通中小学校的数字化转型发展也具有非常重要的意义。该标准拟由三部分构成：

- 第1部分：学校数字基座建设。目的在于规范学校数字基座建设的架构体系；
- 第2部分：数据共享交换。目的在于规范基础教育数字化转型建设中数据共享的交换规则、质量要求、服务要求、安全要求、伦理和隐私；
- 第3部分：应用场景开发。目的在于规范教学、评价、研训和管理等四个应用场景的场景要素和功能要求。



# 基础教育数字化转型建设规范

## 第 2 部分：数据共享交换

### 1 范围

本文件规定了基础教育数字化转型建设中数据共享的交换规则、质量要求、服务要求、安全要求、伦理和隐私。

本文件适用于深圳市、区、校三级数字基座的数据共享交换。

### 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 35273 信息安全技术 个人信息安全规范
- ZWFW C0131 国家政务服务平台统一身份认证隐私保护要求
- DB4403/T 384.2 基础教育管理信息化技术规范 第2部分：数据代码
- DB4403/T 384.5 基础教育管理信息化技术规范 第5部分：数据交换

### 3 术语和定义

下列术语和定义适用于本文件。

#### 3.1

**数据共享 data sharing**

在合法合规的前提下，不同组织、系统或个人之间开放并传递数据资源的行为，旨在促进信息流通、提高数据利用效率和推动协同合作。

#### 3.2

**数据交换 data exchange**

两个或多个系统之间按照预定义的格式和协议自动传输数据的过程，以实现数据的集成、同步或更新。

#### 3.3

**数据脱敏 data anonymization**

通过对个人身份信息或其他敏感信息进行修改或替换，使得数据在保留其价值用于分析或共享的同时，无法直接关联到特定的个人，从而保护个人隐私和数据安全。

#### 3.4

**数据伦理 data ethics**

在数据的收集、处理、分析及利用过程中，根据相关的道德原则和行为规范，确保数据活动的公正性、尊重个体权利、保护隐私、促进社会福祉，防止数据滥用带来的负面影响。

3.5

数据隐私 data privacy

个人对其个人信息（包括但不限于个人身份信息、行为习惯、位置数据等）的控制权以及选择是否公开、如何使用这些信息的权利。

4 数据共享交换规则

4.1 数据内容

数据共享交换的数据内容，参照DB4403/T 384.2进行编码，便于数据共享交换时数据内容的统一。

4.2 数据接口及使用规则

数据共享交换的数据接口及使用，参照DB4403/T 384.5执行。

4.3 数据脱敏原则

数据共享交换的基本数据统一遵循参照ZFW C0131和GB/T 35273对用户脱敏信息的要求执行；自定义数据的脱敏遵循学校数字基座建设脱敏需求和用户提出的脱敏需求。

5 数据质量要求

5.1 数据集成标准

数据集成是稳定高效、弹性伸缩的数据汇聚平台，致力于提供复杂网络环境下、丰富的异构数据源之间高效稳定的数据汇聚融合能力。

5.2 数据集成原则

数据集成主要用于离线（批量）数据汇聚融合处理。通过抽象的不同功能的数据处理器节点编排数据集成流程和作业调度周期，为保障作业的可靠运行，最小粒度可控制单个数据处理器的计算资源消耗和流量控制。数据处理器是对数据操作的抽象，可灵活扩展，支持多种数据源集成、常规处理操作以及自定义脚本处理，从而实现任意结构化、半结构化数据源之间数据传输和转换。

5.3 数据读取和写入标准

数据集成包括读取、转换和写入三类处理器，各处理器之间共享元数据，通过内部管道高效稳定地传递数据。一个集成任务支持多个转换处理器进行数据清洗，并支持多个写入处理器实现多路输出功能。同时针对某些场景，可提供覆盖、去重覆盖、追加、去重追加4种写入模式和增量、全量2种读取模式。

5.4 数据存储标准

数据存储支持时间分区和自定义分区，以支持数据高效读写。依据数据标准定义，对数据分类规整，从而实现对教育数据的层级管理。

5.5 数据集成配置标准

可以通过以下两种模式进行数据集成流程设计配置：

- a) 向导模式：提供向导式的开发引导，通过可视化的引导，快速完成数据集成任务的配置工作，向导模式的学习成本低，但无法支持部分高级功能；



- b) 脚本模式：通过直接编写数据处理脚本来完成数据处理开发，适合高级用户，学习成本较高，脚本模式可以提供更丰富灵活的能力，实现精细化的配置管理。

## 6 数据服务要求

数据服务应遵循数据安全要求，从技术层面提供诸如数据脱敏、黑白名单、接口鉴权、频率限制、类型校验等安全机制来统一保障数据安全，数据服务协议应与在线数据服务保持强一致，在线协议文档应能随数据服务的变更实时更新。应能提供配置化的API数据服务生成方法，包括新增、删除、更新、查询、聚合搜索、批量更新、批量删除等统一的API访问方法，并能依据场景控制各API访问权限。

## 7 数据安全要求

### 7.1 数据分类分级

聘请安全专家根据国家、地方或行业法律法规，结合用户数据分级分类需求和数据资产现状（可借助数据资产梳理系统对学校数字基座资产进行梳理，摸清数据资产情况），开展数据分级分类融标工作，确定数据安全分级分类方案。通过AI算法等技术手段智能标签、数据分级分类规则模型和人工配置数据分级分类规则集的方式对数据表和字段进行数据分级分类标识，形成数据安全分级分类图谱。

### 7.2 数据安全风险评估

结合国家以及行业合规要求对用户整体数据安全风险进行评估。聘请安全专家配合风险测评工具定期从技术、管理、运营等方面进行全面的数据安全风险评估服务，通过数据安全风险评估以及常态化运营保障实现学校数字基座全面的风险以及控制。

### 7.3 数据安全制度体系建设

制定数据安全治理顶层设计，包括内外部策略、部门职责、动态协同等，起到安全治理过程中依据、指引等作用。梳理组织架构、结合合规要求、业务需求、数据资产现状和风险，从组织层面整体考虑和设计，设计包含方针总纲、数据安全管理制度、数据安全操作流程规范、数据安全操作记录/日志的四级数据安全管理体系框架，为数据安全基础管理、数据安全全生命周期管理、数据安全运营各场景管理以及数据安全技术操作提供规范依据。

### 7.4 数据安全运营体系建设

培养/外聘专业的数据安全技术人员进行学校数字基座的安全运营，通过全员安全意识培训、自查整改、安全产品策略运维等服务项目不断发现问题、整改问题，优化补充整个数据安全体系。

### 7.5 数据安全全生命周期防护能力

从数据全生命周期为基座提供安全防护能力，从数据采集、存储、使用、传输、交换、销毁的全生命周期维度进行数据安全的技术防护，结合数据共享交换、数据开放、开发测试、安全运维场景提供完整的技术解决方案。包括数据层的核心数据防护措施和配套安全系统等。所有软硬件设备均需满足数字基座所提出的各项安全功能规范要求。包括但不限于以下要求：

- a) 数据采集安全。应使用数据资产安全管理平台实现学校数字基座基础库数据的梳理以及各类应用上线前的数据合规检查。从资产、数据、行为三个维度对学校数字基座数据资产及风险进行管理。

- b) 数据存储安全。对于学校数字基座中的关键数据需要依据等保相关产品实现国密算法级别数据加密。在此基础上应增加独立于数据库的访问授权机制。任何访问被加密数据的人或应用事先必须经过授权，拥有合法访问权限才能访问加密数据，非授权用户无法访问加密数据，有效防止管理员越权访问及黑客拖库。
- c) 数据使用安全。学校数字基座平台的数据安全审计能力应包含数据库审计能力和 API 调用审计能力。
- d) 数据交换共享安全。学校数字基座平台的数据交换共享安全应具备敏感数据脱敏能力。
- e) 数据传输安全。对于学校数字基座平台的数据传输安全应从数据库协议和网络应用传输协议两方面进行管控。
- f) 数据销毁安全。学校数字基座平台应具备剩余数据定期检索和清理的能力。

## 8 数据伦理和隐私

### 8.1 数据伦理

数据伦理属于科技伦理的范畴，指的是由于大数据技术的产生和使用而引发的社会问题，是集体和人与人之间关系的行为准则问题。作为一种新的技术，大数据技术像其他所有技术一样，其本身是无所谓好坏的，而它的“善”与“恶”全然在于对大数据技术的使用者。一般而言，使用大数据技术的个人、公司都有着不同的目的和动机，由此导致了大数据技术的应用会产生积极影响和消极影响。

学校数字基座建设各方应当主动履行维护国家数据安全和保护公民数据隐私的义务。包括但不限于以下义务：

- a) 不制作、发布或传播危害国家安全、危害社会稳定、违反法律法规的数据信息；
- b) 不窥视、不转让、不传播、不交易违反国家法律法规规定，以及未经用户授权的数据信息；
- c) 自觉维护用户的合法权益，保守用户数据隐私，不得利用用户提供的数据从事任何与向用户作出的承诺无关的活动，不利用技术或其他优势侵犯消费者或用户的合法权益；
- d) 防范计算机恶意代码或破坏性程序的传播，反对制作和传播对计算机网络及他人数据信息系统具有恶意攻击能力的计算机程序，反对非法侵入或破坏他人计算机数据系统；

### 8.2 数据隐私

隐私保护的重要管理制度是三权分立管控制度。三权是指：数据库管理权限、隐私数据安全权限以及审计权限。三个权限分别掌握在不同的管理员手上，三个管理角色的权限相互独立、互不重叠，不允许越权，且相互制衡。

**数据库管理员（DBA）角色：**数据库管理员主要负责系统的维护和管理，数据库设计方案及规划。DBA拥有数据库最高的操作权限。经过隐私保护实施后，数据库中将不包含任何隐私信息。DBA角色能够获取所有的数据但无法读懂隐私信息，DBA无法获取隐私信息保护的策略和密钥信息。

**安全管理员（SA）角色：**是隐私数据保护专用管理角色，主要负责获取隐私信息属性，管理和配置去隐私处理的策略和密钥信息，制定版本更新计划和历史版本归档工作。SA掌握所有去隐私处理使用的策略和密钥，但SA没有访问系统任何主数据库的权限，无法获取隐私信息。

**审计专员角色：**属于4A管理平台的专门的事后审计管理角色，审计专员有权对DBA和SA的任何操作进行审计。一旦发现违规的行为可以及时通告和升级处理。

建立三权分立管控制度的目的就是要建立权力制衡的机制，进一步保证隐私信息的安全。各单位实施过程中，应明确三个角色权限由不同的人员担任，三个角色的权限不能有任何的设置重叠，需配套建立相应版本更新、数据需求、后台运维、日志审计管理流程，要对基座开发及维护人员进行常态化的客

户隐私数据相关安全管理制度及相关知识的宣贯，加强相关人员的安全意识。单位审计员需定期对程序运行日志和用户操作日志进行安全审计和检查工作，并形成正式的审计报告。通过对日志中涉足敏感区域访问的行为以及客户隐私数据的访问日志进行详细分析，初步判断是否危及信息安全，若有安全问题的可疑情况，需及时上报相关领导，并触发后续处理流程。

参 考 文 献

- [1] GB/T 21062.1 政务信息资源交换体系 第1部分：总体框架
  - [2] GB/T 21062.2 政务信息资源交换体系 第2部分：技术要求
  - [3] GB/T 21062.4 政务信息资源交换体系 第4部分：技术管理要求
  - [4] GB/T 21365 信息技术 学习、教育和培训 学习对象元数据
  - [5] GB/T 35274 数据安全技术 大数据服务安全能力要求
  - [6] DB4403/T 384.1 基础教育管理信息化技术规范 第1部分：数据结构
  - [7] DB4403/T 384.3 基础教育管理信息化技术规范 第3部分：教育大数据分析
  - [8] DB4403/T 384.4 基础教育管理信息化技术规范 第4部分：教育用户数据
-