ICS 35.240.90
L67
备案号：

JY

中 华 人 民 共 和 国 教 育 行 业 标 准

JY/T XXXXX-202X

智慧教育平台
学生数据隐私保护通用要求

Smart Educaion System—

General requirements on student information protection

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

202X－XX－XX 发布　　202X－XX－XX 实施

中 华 人 民 共 和 国 教 育 部　　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。

本文件由教育部提出并归口。

本文件起草单位：北京邮电大学、华东师范大学、华南理工大学、阿里技术有限公司、锐捷技术有限公司、广西教育技术和信息化中心、中国电子技术标准化研究院、海康技术有限公司、新华三科技有限公司等。

本文件主要起草人：李青，钱冬明，沈雄，彭俊涛，卢海燕，杜婧，余云涛，于翠波，苏明雪，康蓓等。

智慧教育平台 学生数据隐私保护通用要求

1. 范围

本文件规定了教育领域中学生数据隐私保护的基本原则和保护要求。

本文件适用于教育信息系统中学生数据隐私保护相关业务。

2. 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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 35273-2020 个人信息安全规范

儿童个人信息网络保护规定

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

3. 术语和定义

下列术语和定义适用于本文件。

3.1

教育数据 education information

反映教育活动状态及其变化的实质性内容的数据。

[改写自GB/T 36618-2018]

3.2

个人信息 personal information

以电子或其他方式记录的能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的各种信息。

[来源：GB/T 35273-2020 ，术语和定义 3.1]

3.3

个人信息主体 personal information subject

个人信息所标识或者关联的自然人。

[来源：GB/T 35273-2020 ，术语和定义 3.3]

3.4

个人信息控制者 personal information controller

有能力决定个人信息处理目的、方式等的组织或个人。

[来源：GB/T 35273-2020 ，术语和定义 3.4]

3.5

明示同意 expicit consent

个人信息主体通过书面、口头等方式主动作出纸质或电子形式的声明，或者自主做出肯定性动作，对其个人信息进行特定处理作出明确授权的行为。

[来源：GB/T 35273-2020 术语和定义 3.6]

3.6

授权同意 consent

个人信息主体对其个人信息进行特定处理作出明确授权的行为。

[来源：GB/T 35273-2020 术语和定义 3.7]

3.7

数据隐私保护 privacy protection

从数据角度对个人隐私权的保护措施。学生数据隐私保护的对象包括但不限于：出生日期、联系方式、健康状况、家庭住址、家庭财政情况、家庭成员、学历、工作经历等等。

3.8

教育应用 education application

以信息化形式提供教育服务的软件产品，可以是系统平台、工具、应用软件手机App等多种形式。

4. 基本原则

4.1 概述

GB/T 35273-2020 第4条规定的个人信息安全基本原则适用于本文件，包括责权一致、目的明确、选择同意、最小必要、公开透明、确保安全、主体参与。除此之外，教育应用中隐私保护还应遵循一些其他基本原则，包括使用限制原则和问责原则。

4.2 使用限制原则

个人信息不应被公开，或被用于明确收集目的以外的情形，除非：数据主体同意，或法律要求。

4.3 问责原则

数据控制者应对符合上述各原则的方式方法负责。

5. 保护要求

5.1 隐私政策

隐私政策是各教育信息化系统以及系统所在的机构保护用户个人隐私的声明文件。数据隐私保护评价方面关注度集中在隐私政策的内容是否符合法律规定以及是否全面上。不仅要对隐私政策的基本情况（告知形式等）进行评价，还要对隐私政策的整体内容进行评价。

5.1.1 制定情况

5.1.1.1 一般性隐私政策

教育应用个人信息控制者应制定和在显著的地方声明其用户隐私政策。

5.1.1.2 儿童隐私政策

教育应用个人信息控制者应为儿童用户或教育应用中所涉及的儿童信息专门制定和声明隐私政策。

5.1.1.3 隐私政策同意

教育应用个人信息控制者在告知隐私政策时，应征得用户的明示同意。对于14周岁及以下的未成年用户应强调要征得其监护人的同意。

5.1.1.4 隐私政策易访问度

教育应用个人信息控制者应保障用户较为容易地查看隐私政策。从首页面开始查看隐私政策时，需点击（或其他操作）的次数应在4次（含）以内。隐私政策文件使用中文简体，字体和版式应当清晰，并且易于阅读。

除了在登录或注册界面展示隐私政策内容或链接以外，以及通过咨询客服等方式以外，还应通过其他多种方式提供隐私政策内容，包括但不局限于在帮助说明文档中列出，在官方网站中列出等。教育应用对于隐私政策的展示应该在不同版本中保持一致，不得频繁变更展示路径，或故意隐藏隐私政策内容的访问路径。

5.1.1.5 隐私政策更新

隐私政策发生变更时，教育应用个人信息控制者应及时通过电子邮件、推送通知等方式告知学生/监护人。

5.1.2 具体内容

5.1.2.1 信息收集和使用

隐私政策中应明确规定学生信息收集和使用的目的、方式、范围，且信息收集和使用的目的应与促进学生学习相关。

5.1.2.2 信息存储

隐私政策应明确规定学生信息的存储地点、存储期限、超出期限的处理方式、数据出境情况的处理规则。

5.1.2.3 信息披露、转让与共享

隐私政策应明确规定学生信息披露、转让与共享的目的和信息类型，接收学生信息的第三方类型以及第三方保护学生信息的方式。

5.1.2.4 学生及监护人权利保障

隐私政策中应明确规定学生及其监护人对学生信息进行处理的权利和实现机制，如查询途径、删除途径、更正途径、注销账户的途径、撤回授权同意的途径、维权投诉的途径等。

5.1.2.5 安全保障

隐私政策中应写明教育应用采取的学生信息安全保护措施和技术，如身份鉴别、数据加密、访问控制、去标识化等。

5.1.2.6 联系方式

隐私政策中应写明该教育应用的联系方式。

5.2 信息处理周期

本文件将信息处理周期分为信息收集，信息使用，信息存储，信息披露、转让与共享七个步骤，每个步骤的具体要求如下。

5.2.1 信息收集

5.2.1.1 信息收集的范围

教育应用个人信息控制者在收集学生信息时，应遵循最小必要原则，仅收集业务功能所必需的信息，不得收集与业务功能无关的信息。

5.2.1.2 信息收集同意

教育应用个人信息控制者在收集学生信息时，应以明显的方式告知学生并征得其同意，对于14周岁及以下的未成年人应征得其监护人的同意。

5.2.1.3 额外信息收集

教育应用个人信息控制者收集的学生信息超出其隐私政策所述信息收集范围时，应再次征得学生同意，对于14周岁及以下的未成年人应再次征得其监护人的同意，且收集信息的目的应与促进学生学习相关。

5.2.1.4 拒绝信息收集

学生/监护人拒绝特定业务的信息收集后，教育应用个人信息控制者不应暂停学生自主选择使用的其他业务功能，或降低其他业务功能的服务质量。

5.2.1.5 信息收集与功能捆绑

教育应用个人信息控制者在收集学生信息时，不应通过捆绑产品或各项业务功能的方式，要求学生一次性授权同意其未申请或使用的业务功能收集个人信息的请求。

5.2.1.6 信息收集与活动捆绑

在学生申请参加教育应用组织的活动（学科竞赛等）时，教育应用个人信息控制者不应以此为由收集合理范围之外的信息。

5.2.2 信息使用

5.2.2.1 信息使用范围

教育应用业务功能实际所使用的学生信息类型，应在其收集个人信息时所声明的范围之中，确需超出上述范围使用个人信息的，应再次征得学生的同意，对于14周岁及以下的未成年人应再次征得其监护人的同意。

5.2.2.2 广告与营销

教育应用不应将收集到的学生信息用于广告与营销等商业目的。

5.2.3 信息存储

5.2.3.1 公共信息处理

学生账户注销后，教育应用在删除学生个人信息的同时，应将学生在论坛、评论区等产生的数据应予以匿名化处理或删除。

5.2.3.2 教育应用停止运行

教育应用停止运营产品或服务的，应立即停止收集学生的个人信息，删除已收集的儿童个人信息，并将停止运营的通知及时告知学生及其监护人。

5.2.4 信息披露、转让与共享

教育应用个人信息控制者在披露、转让、共享学生个人信息时，应征得学生及其监护人的同意。

5.3 用户权利保障

5.3.1 信息查询

教育应用个人信息控制者应为学生/监护人对已收集的学生个人信息的查询提供途径。

5.3.2 信息更正

5.3.2.1 信息更正途径

教育应用个人信息控制者应为学生/监护人对已收集的学生个人信息的更正提供途径。

5.3.2.2 信息更正期限

学生/监护人提出学生个人信息更正请求后，教育应用个人信息控制者应在15个工作日内处理请求。

5.3.3 信息删除

5.3.3.1 信息删除途径

教育应用个人信息控制者应为学生/监护人对已收集的学生个人信息的删除提供途径。

5.3.3.2 信息删除期限

学生/监护人提出学生信息删除请求后，教育应用个人信息控制者应在15个工作日内处理请求。

5.3.4 撤回授权同意

5.3.4.1 撤回授权同意途径

教育应用个人信息控制者应为学生/监护人撤回信息收集授权提供途径。

5.3.4.2 撤回授权同意处理

学生/监护人撤回授权同意后，教育应用个人信息控制者应立即停止收集相关信息。

5.3.5 注销账户

5.3.5.1 注销账户途径

教育应用个人信息控制者应为学生/监护人提供注销账户的途径。

5.3.5.2 注销账户处理

学生/监护人在注销账户后，教育应用个人信息控制者应删除或匿名化处理学生的个人信息。

5.3.6 投诉举报

5.3.6.1 投诉举报途径

教育应用个人信息控制者应为学生/监护人提供投诉举报的方式，包括但不限于电子邮件、客服电话、在线客服等。

5.3.6.2 投诉举报处理期限

学生/监护人发起投诉举报后，教育应用个人信息控制者应在15个工作日内处理投诉举报。

5.4 信息安全保障

安全保障是贯穿整个信息保护过程的重要保障，在法律法规中对教育应用采取的安全技术措施、安全管理措施等做出了具体规定。数据隐私保护中对信息安全保障的通用要求应遵循GB/T 35273-2020的规定。

教育机构作为个人信息控制者应根据有关国家标准的要求，建立适当的数据安全能力，落实必要的管理和技术措施，确保数据处于有效保护和合法利用的状态，防止个人信息的泄漏、损毁、丢失、篡改。

5.4.1 制定数据隐私保护管理制度

教育个人信息控制者应制定本单位的个人信息管理办法，规范数据分类分级，明确安全防护措施，建立数据安全应急处理措施。

5.4.2 对个人信息实行分类分级

教育个人信息控制者应全面梳理本单位的梳理，形成数据资源目录，根据行业的分类分级工作指南，确定重要数据的目录，对列入目录的数据进行重点保护。

5.4.3 提升个人信息数据安全防护水平

教育个人信息控制者应遵从数据安全法和数据隐私保护等相关法律法规的防护要求、提升个人信息防入侵、防泄露、防滥用、防损毁能力。

5.4.4 规范个人信息开放共享

教育个人信息控制者应建立个人信息开放共享审批与审核机制，加强数据的开放共享属性和防护要求，对开放共享过程进行审计与监测。

5.4.5 开展个人信息数据安全意识培训

教育个人信息控制者应定期组织数据安全意识培训，提升个人信息数据安全意识和防护能力。