

# 保定幼儿师范高等专科学校

校信字【2026】1号

## 保定幼儿师范高等专科学校 个人信息保护管理制度

### 第一章 总则

#### 第一条 制定目的与依据

为全面规范我校个人信息安全管理工作，筑牢全校师生，特别是未成年学生，以及学生家长的个人信息安全防线，有效防范个人信息过度收集、违规共享、泄露篡改、非法利用等各类安全风险，全方位压实个人信息保护主体责任，切实保障广大师生合法权益，依据《中华人民共和国网络安全法》、《中华人民共和国个人信息保护法》、《中华人民共和国刑法》、《中华人民共和国治安管理处罚法》、《中华人民共和国居民身份证法》、《网络数据安全条例》、《人脸识别技术应用安全管理规定》、《APP违法违规收集使用个人信息行为认定办法》及GB/T35273-2020《信息安全技术个人信息安全规范》等法律法规、国家标准及教育系统专项治理工作要求，结合我校实际情况，制定本管理制度。

## **第二条 适用范围**

本制度适用于学校所有教职员工、全体在校学生、学生监护人，以及所有与学校开展合作服务配套的第三方机构及工作人员。覆盖学校所有个人信息处理相关活动，包括但不限于个人信息收集、录入存储、加工使用、共享传输、对外提供、公开公示、销毁删除、安全运维、应急处置、合规审计等全环节；涵盖学校官方网站、校园专属 APP、微信公众号及小程序、学校所有信息化平台，线下校园办事窗口。

## **第三条 核心管理原则**

学校个人信息保护工作坚决杜绝超范围、非必要过度收集个人信息，严格规范未成年人个人信息处理流程，严控第三方机构使用校内人员个人信息及权限，全面落实人脸识别等生物识别技术合规应用要求，全方位筑牢校园个人信息安全防护屏障，确保个人信息处理全程合法合规、安全可控。

# **第二章 组织管理与岗位职责**

## **第四条 专项管理工作领导小组**

依托学校网络安全与信息化工作委员会，成立个人信息保护专项管理工作领导小组，由学校党委书记、校长担任组长，主管副校级领导任常务副组长，各职能处室、系部主要负责人为小组成员，主要职责为统筹安排全校个人信息保护治理工作，审定学

校个人信息保护相关规章制度，包括年度工作计划及应急处置预案，统筹协调、风险管控、违规处理等问题，督促各部门、各岗位落实个人信息保护主体责任，定期对接教育主管部门、网信、公安等监管单位，配合开展专项检查、合规核查及整改落实工作。

### **第五条 岗位责任与追责机制**

严格落实个人信息保护一岗双责制，学校各级负责人为对应管辖范围内个人信息保护第一责任人，岗位经办人员为直接责任人。所有涉及个人信息处理的工作人员须签订个人信息安全保密责任书，明确岗位职责、操作规范及违规责任。对未落实本管理制度、违规处理个人信息、造成信息泄露、篡改、丢失或引发不良影响及安全事故的，依规追究相关人员行政责任、岗位责任；情节严重触犯法律法规的，依法移交司法机关追究法律责任。

## **第三章 个人信息分类处理与合规管控**

### **第六条 个人信息分级分类管理**

学校按照国家标准及教育行业数据管理要求，对所有个人信息实行分级分类管理，划分为普通个人信息和敏感个人信息两类。普通个人信息包含教职工及学生姓名、性别、学号、工号等基础识别信息；敏感个人信息重点包含居民身份证号码、联系方式、家庭住址、银行卡号、家长职业信息、人脸指纹等生物识别信息、学籍核心私密信息，以及未成年学生个人信息。所有敏感

个人信息实行提级保护，严禁随意调取、使用及传播。

### **第七条 未成年人个人信息专项处理规则**

针对学校大量未成年学生个人信息处理工作，学校单独制定相应管理办法，设置专门的家长沟通平台，明确未成年个人信息收集范围、使用用途、存储期限、保护措施、销毁规范及监护人沟通机制。处理未成年学生个人信息前，必须严格履行**双知情同意程序**。严禁未经监护人同意，擅自收集、使用、共享未成年学生个人敏感信息，严禁以教育管理名义违规采集未成年学生非必要生物识别信息。

### **第八条 个人信息收集最小化管控要求**

全校各部门、各信息化平台及线下办事窗口收集个人信息严格遵循“必要够用、非必要不收集”原则，坚决整治过度收集违规问题。严禁超工作履职、教育教学、学籍管理、家校服务必备范围，违规收集学生学籍冗余信息、家长身份证号、私人联系方式、家长职业等非必要个人信息；校园各类 APP、小程序、线上办事系统不得强制索要非业务必需的个人权限及个人信息，不得设置不授权无法使用基础服务的强制门槛。所有个人信息收集实行事前审批备案，新增信息收集事项须经个人信息保护专项领导小组审核同意后方可实施，从源头杜绝过度收集、违规采集乱象。

## **第四章 第三方合作与信息共享管理**

## **第九条 第三方机构准入与协议管控**

学校与校外培训机构、信息化技术服务商、实训合作企业、家校服务合作单位等第三方机构开展业务合作，涉及向第三方提供师生及监护人个人信息的，实行严格准入审核与合规协议管理。所有合作第三方机构必须与学校签订专项个人信息安全保密合作协议，明确第三方个人信息处理权限、使用范围、处理目的、存储期限、安全防护责任、严禁二次共享、违规追责及信息泄露赔偿条款，未签订合规协议、未通过安全评估的第三方机构，一律不得接触、获取、处理学校任何个人信息。

## **第十条 信息共享告知与知情同意流程**

学校向任何第三方机构提供个人信息前，必须严格履行双重告知与同意程序。提前向对应个人信息主体（教职工、成年学生、未成年学生监护人）精准告知合作第三方机构具体名称、合作业务内容、个人信息处理具体目的、处理方式、信息使用期限及安全保护措施，明确告知信息主体享有的查询、更正、撤回同意、删除信息等合法权利。必须取得个人信息主体自愿书面或实名认证线上同意后，方可向第三方传输、提供相关个人信息，严禁未告知、未取得同意擅自向第三方流转、共享、外泄个人信息。

## **第十一条 第三方全程监管与退出处置**

学校归口管理部门对合作第三方机构个人信息处理活动实行全程动态监管，定期开展第三方合规抽查、安全隐患排查及履职情况核查，建立第三方机构个人信息保护信用台账，对违规操

作、防护不到位的第三方机构立即暂停合作、限期整改，整改不合格的坚决终止合作并依法追责。合作终止后，督促第三方机构立即停止个人信息使用，全部销毁或返还学校所提供的个人信息，不得私自留存、备份、复用相关信息，全程做好处置记录并归档留存，确保第三方合作全流程信息安全闭环管理。

## **第五章 生物识别与线下场景安全管理**

### **第十二条 人脸识别技术合规应用管控**

学校校园门禁、考勤打卡、场馆出入、实训场地管理等线下场所，如需应用人脸识别等生物识别技术，严禁违规滥用人脸识别技术。非校园安全、日常管理必需场景一律不启用人脸识别应用，确需使用人脸识别的，必须专项报备、合规审批，明确采集使用范围、存储周期及防护措施，人脸生物信息实行本地加密存储，严禁云端随意上传、对外共享泄露。严禁在学生宿舍、教学课堂、日常活动区域违规增设人脸识别采集设备，严控生物识别信息采集、使用、留存全流程安全。

### **第十三条 线下场景日常安全防护规范**

学校各线下办公窗口、学生管理站点、学籍办理场所、后勤服务网点等线下场景，规范个人信息纸质材料、电子资料管理，纸质涉密个人资料单独专柜上锁存放，电子信息设备设置专人账号密码管控，离岗及时锁屏关机。线下办理业务收集的个人信息

表单、资料台账定期归档，废弃含个人敏感信息的纸质材料、电子存储介质，按照保密规范统一销毁处置，严禁随意丢弃、私自外传。各线下场所定期开展个人信息泄露隐患自查，及时整改台账管理不规范、保管不到位、操作不合规等问题，筑牢线下场景信息安全防线。

## **第六章 安全防护、审计与应急处置**

### **第十四条 常态化安全保护技术与管理措施**

学校全面落实个人信息常态化安全保护措施，健全校园信息系统网络安全防护体系，对存储个人信息的服务器、业务系统、数据库实行加密存储、访问权限分级管控、防火墙防护、安全漏洞定期检测修复。规范个人信息操作全流程日志记录，所有信息调取、修改、共享、删除操作全程留痕，审计日志留存时长严格按照规范不少于180天，确保所有操作行为可溯源、可核查、可追责。定期开展个人信息安全风险自查、隐患排查及安全测评，及时整改信息泄露、权限失控、防护薄弱等各类风险隐患，常态化更新安全防护策略。

### **第十五条 合规培训与宣传教育工作**

学校定期组织全校教职工、管理人员、第三方合作工作人员开展个人信息保护合规专项培训，讲解相关法律法规、本管理制度条款及违规处置案例，提升全员合规管理和安全防护意识。面

向在校学生及学生监护人，通过主题班会、家校通知、校园宣传、线上科普等多种形式，开展个人信息安全宣传教育，普及个人信息保护常识，引导师生及监护人增强信息安全防范意识，主动抵制个人信息违规收集、随意泄露等不良行为。

### **第十六条 信息泄露应急处置与整改问责**

学校建立个人信息安全事件应急预案，明确信息泄露、篡改、丢失等安全事件预警、上报、处置、整改、善后全流程工作流程。一旦发生个人信息安全泄露及违规事件，第一时间启动应急预案，快速采取阻断泄露、隐患排查、信息补救、风险管控等处置措施，及时告知受影响的个人信息主体，按规定时限上报教育主管部门、网信及公安监管单位。对事件原因深度复盘核查，从严追责相关责任人员，全面落实整改措施，健全长效防控机制，杜绝同类安全问题重复发生。

## **第七章 附 则**

### **第十七条 制度修订与配套细则**

本管理制度根据国家法律法规更新、上级教育主管部门专项治理工作要求及学校校园管理实际情况，由保定幼儿师范高等专科学校网络安全与信息化工作委员会适时修订完善。学校各相关职能部门可依据本制度，结合分管工作实际，制定个人信息保护配套实施细则、操作流程及岗位工作规范，确保制度落地见效、

贴合实操管理需求。

### **第十八条 生效日期与解释权限**

本管理制度自发布之日起，由保定幼儿师范高等专科学校网络安全与信息化工作委员会负责统一解释。

保定幼儿师范高等专科学校  
网络安全与信息化工作委员会  
2026年6月2日

