青岛职业技术学院数据管理办法

第一章 总则

第一条 为加快学校数字化转型，全面加强学校数据的规范管理，提升学校治理能力和服务水平，充分发挥数据在学校建设中的重要作用，依据《中华人民共和国数据安全法》《山东省电子政务和政务数据管理办法》《青岛市公共数据管理办法》等相关法律法规政策，结合学校实际，制定本办法。

第二条 本办法所称数据是指学校各部门在教学、科研、管理、服务等工作中通过信息化系统、信息化手段以及相关管理平台采集、存储或使用的各类信息记录，不包括用于科学研究活动的原始数据及衍生数据。

涉密数据管理，按照相关标准和规定执行。

第三条 数据管理是指对上述数据进行采集、汇集、存储、共享、使用、维护及安全管理等工作。

第四条 数据管理应当遵循以下原则。

（一）统一标准、归口管理原则。学校应当依据国家、教育部、行业等制定的相关标准和规范，并根据学校实际制定、完善统一数据标准。各部门依据学校统一数据标准规范提供数据，确保数据真实、准确、完整、及时、有效。

（二）分类分级、安全共享原则。各部门应当按照业务类别及数据重要、敏感程度等进行数据分类并分级保护和共

享。按照“谁收集谁负责、谁持有谁负责、谁管理谁负责、谁使用谁负责”的工作机制确定安全责任。

（三）一数一源，数据公有原则。各部门应当遵照“一数一源”的原则确定数据权威来源。数据是学校公共资源，所有权和使用权归学校所有。各部门应当遵照“一次采集，重复使用”原则，开展数据采集、存储、共享和使用。

第二章 职责分工

第五条 学校网络安全与信息化领导小组（以下简称网信领导小组）是学校数据管理的领导机构，负责顶层设计、政策制定和学校数据管理等重大事项决策。

第六条 信息技术中心负责数据管理日常工作，包括校级数据中心的建设与管理、制定数据标准、汇总编码规范、数据安全审计等工作。

信息技术中心应当每学期向网信领导小组汇报数据管理工作。

第七条 学校各部门为相关领域数据管理的主责部门，应当落实数据管理的各项工作要求，包括执行数据标准、提升数据质量、促进数据共享，完善数据安全措施等工作，并按要求向校级数据中心提供权威数据。

第三章 数据分类分级

第八条 基于学校业务类型，对数据进行分类管理。

（一）基本信息类

1.教师数据。教职工基本信息、入职、离校、职称评聘、考核、培训、奖惩、薪资、党团关系、出国（境）出访以及离退休等相关数据。

2.学生数据。学生（含国际学生）基本信息、迎新、奖惩、奖学金、助学金、贷款、党团关系、毕业、就业、离校、校友、生活等相关数据。

（二）业务数据类

1.教学数据。所有与学生（含国际学生）相关的招生、学籍、教学计划、排课、选课、成绩、实习实训等；学生评教、教学改革、专业、课程、教学资源等；教育（合作）培训、校企（政）合作相关数据。

2.科（教）研数据。科（教、思政）研项目管理、科（教）研合同管理、各类成果管理、科研机构管理、科研平台、科（教）研团队、科（教）研经费管理、科（教）研业绩考核等相关数据。

3.财务数据。财务管理、经费管理、教职工薪资发放、学生收费信息、消费支付等。

4.资产数据。采购管理、固定资产管理（含图书文献资料）、实验室管理、设备管理、房产管理、土地管理等相关数据。

5.行政管理数据。组织机构、党团群组织、行政办公、教育合作、学生档案管理、文件档案管理、科研档案管理等相关数据。

6.公共数据。校园一卡通、校园网络服务、门禁信息、网站信息、电子邮件、水电气能耗、车辆信息、安全保卫后勤服务及其他服务数据。

第九条 基于数据重要性、敏感性、影响对象及程度确定数据等级，对数据进行分级管理。

（一）第一级数据（公开数据），是指学校依规定公开的学校基本信息、数据标准、代码信息及相关数据。

（二）第二级数据（内部数据），是指不予公开，但可在一定范围内共享的数据，包括各部门、二级学院按照职能收集并为教学、科研、管理决策等提供支撑的数据。

（三）第三级数据（敏感数据），是指涉及学校秘密、个人敏感信息的相关数据，一旦遭篡改、泄露、丢失、损毁后，对学校、个人安全或利益造成损害的数据。

（四）第四级数据（高敏数据），是指一旦遭篡改、泄露、丢失、损毁后，对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成严重损害的数据。

各部门应当根据分级要求确定数据等级，并报信息技术中心备案。确定为第四级数据的，经信息技术中心审核后，报学校网信领导小组审定。

第四章 数据采集

第十条 各部门应当按照部门工作职能制定数据目录，数据目录需包括具体的数据责任人和数据更新周期等信息，信息技术中心应当参照数据标准及各部门数据目录，汇总制定《数据目录》，并通过校级数据中心平台发布。

第十一条 各部门应当按照《数据目录》及时采集数据，并提供给校级数据中心，凡属于校级数据中心可以获取的数据，原则上不得重复采集。

第十二条 《数据目录》实行定期更新维护制度。信息技术中心负责协同各部门制定《数据目录》各数据项的具体更新周期，各部门应当按更新周期要求进行《数据目录》更新维护。

第十三条 信息技术中心应当通过校级数据中心平台对各部门采集提供的数据进行质量检测，同时通过师生个人数据中心等功能模块对师生开放个人数据。

各部门应当根据质量检测结果和师生反馈从业务系统源头修改、完善数据，提升数据质量，发挥数据价值。

第五章 数据共享使用

第十四条 校级数据中心是学校数据的集中存储、整合、共享交换平台（对应智慧校园平台中的“数据中台”）。

《数据目录》为学校各部门间数据共享交换依据。

第十五条 结合数据分级情况，数据应当按照如下类型共享：第一级数据为公开类，在学校官网发布；第二级数据为审核共享类，须经审核后共享；第三级数据为有条件共享类，需进行脱敏或加密后共享；第四级数据为不共享类，因工作需要确需共享的，应当经学校网信领导小组批准。

第十六条 各部门应当按照“谁主管、谁提供、谁负责”的原则，确定提供数据的共享类型，及时提供、维护和更新共享数据，保证共享数据的完整性、准确性、时效性、标准性。

第十七条 各部门之间的数据共享应当通过线上流程审批并经校级数据中心提供。各部门应当根据“按需够用”原

则申请数据，填报《数据使用审批单》（附件 1）经数据提供部门审核同意后，根据数据处理工作量大小，在 1-5 个工作日内通过校级数据中心以线上方式提供所申请的数据。

第十八条 数据使用部门不得超出申请范围使用共享数据，不得以任何方式用于社会有偿服务或其他商业活动，并对共享数据的滥用、非授权使用、未经许可的扩散以及泄露等行为及后果承担相应责任。数据使用中涉及第三方单位的，应当按要求与第三方签订《数据共享保密协议》（附件 2）。

第六章 数据安全

第十九条 各部门应当定期对数据进行安全检查，加强业务系统安全防护，建立应急处置、备份恢复机制，保障数据和平台安全、可靠运行，杜绝越权访问、错误授权等不当行为。

第二十条 数据按照四种级别进行分级管控。

（一）第一级管控，实施基本的内部安全管理措施和基本的数据全生命周期安全管理。

（二）第二级管控，实施必要的内部安全管理措施、审批制度及应急处置措施。将相关安全责任落实到项目负责人，签订负责人安全承诺。实施必要的数据全生命周期管理，采用必要的技术措施保障数据安全，建立准实时安全预警机制。

（三）第三级管控，实施严格的内部安全管理措施、审批制度及应急处置措施。将相关安全责任落实到接触数据个人，签订个人安全承诺。实施严格的数据全生命周期管理，

采用严格的技术措施保障数据安全，建立准实时安全预警机制。

（四）第四级管控，实施最严格的内部安全管理措施、审批制度及应急处置措施。将相关安全责任落实到接触数据个人，签订个人安全承诺。实施最严格的数据全生命周期管理，采用严格的技术措施保障数据安全，建立实时安全预警机制。

第二十一条 信息技术中心在学校网信领导小组指导下协调数据管理全过程的安全保障工作，防止未经授权的数据活动，开展数据安全风险评估、安全管理审查、安全质量考核及安全宣传教育，推进常态化数据安全监管机制。

第二十二条 学校各部门数据采集应当根据有关法律法规，制定涵盖数据采集、应用、开放、共享、安全等实施细则，明确责任人，开展数据风险评估，落实安全管理责任制。

第二十三条 建立健全数据脱敏脱密处理机制，确需在非保密环境下使用的涉及国家安全、社会公共利益、商业秘密的数据依法进行脱敏脱密处理。

第七章 数据管理监督与考核

第二十四条 各部门及个人违反本办法规定，有下列情形之一的，由学校网信领导小组根据实际情况责令限期改正。造成严重不良后果的，按照相关规定予以追责:

（一）未按规定开放或使用数据的;

（二）提供数据目录和数据内容的质量不达标的，或未按照规定时限发布、更新数据目录和数据内容的;

（三）数据使用管理失控，致使出现滥用、盗用及泄漏的；

（四）未经授权，擅自将学校数据用于本部门履行职责所需范围以外的，或擅自转让给第三方的，或利用学校数据开展经营性活动的；

（五）封锁、瞒报数据安全事件，拒不配合有关部门依法开展调查、处置工作，或者对有关部门通报的问题和风险隐患不及时整改并造成严重后果的。

第二十五条 数据管理工作纳入学校考核，信息技术中心负责制定考核办法，对职能部门的业务信息系统覆盖率情况，数据目录制定、完善和更新情况，以及信息化系统的数据共享、更新和有效性情况进行考核。每学期发布一期学校数据质量报告。

第二十六条 对于违反法律、法规和学校相关规定，造成国家、学校和个人损失的，将按程序依法依规追究相关单位及个人的责任。

第八章 附则

第二十七条 本办法自印发之日起开始施行，原《青岛职业技术学院信息化数据资源暂行管理办法》（技术学院综发〔2019〕1号）同时废止。

附件：1.青岛职业技术学院数据使用申请表

2.青岛职业技术学院数据共享保密协议

附件 1

青岛职业技术学院数据使用申请表

申请部门		申请时间	
申请内容			
用　　途			
负 责 人		联系电话	
经 办 人		联系电话	
部门承诺	我部门承诺遵守学院数据管理办法规定，不将所申请使用的数据资源用于申请授权范围以外用途，对提供的数据保密,不向第三方提供，不损害用户隐私权等权益。 部门负责人签字:　　公章: 年　　月　　日		
信息技术中心意见	负责人签字:　　公章: 年　　月　　日		
数据提供部门意见	负责人签字:　　公章: 年　　月　　日		

填表说明：只有申请使用有条件共享数据资源时才需数据提供部门审批。

附件 2

青岛职业技术学院数据共享保密协议

为做好我校数据管理工作,保障数据安全和合理使用,特签订本协议。

一、签约双方

甲方：信息技术中心

乙方（数据使用方）:

二、保密的内容和范围

甲方从数据中台提供的数据。

三、乙方保密责任

1.乙方保证数据安全，防止任何形式泄露数据。

2.乙方不能将所申请使用的数据用于申请授权范围以外用途。

3.如乙方造成数据泄密等问题，一切后果由乙方承担。

四、本协议一式两份，自签订之日起生效。

甲　方（公章）:　　乙　方（公章）:

负责人（签字）:　　负责人（签字）:

日期:　　年　　月　　日　　日期:　　年　　月　　日

青岛职业技术学院师生个人信息保护管理办法

第一章　总则

第一条　为保护学校师生个人信息（以下简称个人信息），明确责任，建立个人信息全流程管理制度，切实维护广大师生的合法权益，依据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》及相关国家标准，结合学校实际，制定本办法。

第二条　本办法所称个人信息是指以电子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。

本办法所称敏感个人信息是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

第三条　本办法适用于在教育教学、科研、管理、服务等活动中涉及学校师生个人信息的全生命周期管理。具体指在学校信息化建设中，为满足学校教学、科研及管理服务需求，学校师生有义务提供相关个人信息，在符合国家及相关主管部门在学籍、教务、人事、财务、档案、设备、资产管理等方面的法律法规及规章制度要求时，可依照本办法处置个人信息。

第四条　个人信息保护应当遵循合规合法、最小必要、知情同意、公开透明、目的明确、确保安全、责任明确的原则，

实行“谁采集谁负责、谁使用谁负责、谁发布谁负责”的工作机制。

第二章 组织机构及职责

第五条 学校网络安全与信息化领导小组（以下简称“网信领导小组”）是个人信息保护的领导机构，负责个人信息保护工作的顶层设计、统筹规划、协调推进和指导监督。

第六条 信息技术中心负责落实网信领导小组决议，制定规章制度，协调应急处置，进行个人信息整体防护。

第七条 各信息化数据的主管部门（以下简称数据主管部门）负责具体落实本部门管理的个人信息的安全保护工作。部门负责人应当严格落实学校规定，明确操作权限，排查、处置和报告个人信息泄露事件。

第八条 学校师生为其个人信息的所有者。师生应当主动更新、妥善保管个人信息，确保信息准确、完整和安全。由于师生个人原因造成的个人信息泄露、损坏、丢失，由本人承担相应责任；对他人个人信息造成不良影响的，将依据本办法及有关法律法规政策追究相关人员的责任。

第三章 个人信息收集

第九条 学校信息化建设中的个人信息采集，由相关数据主管部门负责。数据主管部门原则上应当把相关业务系统作为数据源系统，非必要不允许线下采集并避免重复收集。未经网信领导小组批准，学校任何部门和个人不得收集敏感个人信息或超出职能范围的个人信息。

第十条 收集个人信息应当遵循最小必要原则，收集时需明示目的、方式、范围和期限，并经同意后方可收集。

第十一条 数据主管部门应当定期审核和更新个人信息，确保个人信息的准确性和完整性。

第十二条 为维护公共安全所必需在公共场所安装的个人身份识别图像采集设备，应当遵守国家有关规定设置显著的提示标识。所采集的个人图像、身份识别信息只能用于维护公共安全的目的，不得用于其他目的。

第四章 个人信息存储和传输

第十三条 学校数据中台是个人信息集中统一的存储平台。数据主管部门采集到的个人信息，除存储在相关的业务系统数据库中，应当按照学校数据管理规定，将采集到的个人信息提交到学校的数据中台。

个人信息不得在校外或非全域数据中心存储。

第十四条 个人信息存储期限应为实现处理目的所必需的最短时间，超期信息应当按要求归档或销毁。敏感个人信息应当采用符合国家要求的算法加密存储。

第十五条 个人信息的存储系统和设备应当具备备份和恢复功能，确保存储安全。

第十六条 敏感个人信息在校园网内部不同部门间传输，或向校外合作单位传输时，必须采用加密技术保障传输安全，防止信息泄露与篡改。不得通过即时通讯软件、电子邮件系统和移动存储介质传输敏感个人信息。

第五章 个人信息使用

第十七条 需要使用个人信息的项目，应当根据项目需求，按照最小化原则提报数据使用申请，通过学校数据中台在线接口方式获取，实行“用而不存”，并签订数据安全承诺书，严禁将个人信息挪作他用。数据主管部门应采取“最小授权”策略提供个人信息。

第十八条 因信息化建设工作需要，可接触到个人信息的相关人员负有保密责任，严禁未经授权对外提供个人信息。

第十九条 因工作需要向校外第三方共享师生个人信息，相关责任部门应当与第三方签订数据安全和保密协议，明确第三方责任义务。

第二十条 个人信息不得用于商业用途，各部门需要使用个人信息开展统计分析、科研、决策分析时应当对个人信息进行脱敏处理。

第二十一条 个人信息原则上不得公开，确需公开的应当遵循最小化原则，公示去标识化后的相关信息。

第二十二条 原则上不得向境外提供个人信息，确需提供的应当事前进行个人信息保护影响和合法性评估，确保数据出境安全。

第六章 个人信息删除

第二十三条 注销信息系统应确保个人信息数据已清理。违反规定收集、使用的个人信息，应当依法依规及时删除。

第二十四条 报废存储设备时，存储过个人信息的物理介质，如硬盘、U 盘等，需采用消磁、物理粉碎等专业手段彻底销毁数据。

第七章 安全保障及责任追究

第二十五条 各数据主管部门应当将个人信息保护纳入网络安全管理体系，主要负责人为第一责任人，信息系统管理员为直接责任人。

第二十六条 信息技术中心应当协同各数据主管部门对涉及师生个人信息处理的工作人员开展定期安全培训，签订保密协议，明确违规处理个人信息的法律责任，提高工作人员安全意识与操作技能。

第二十七条 发生个人信息泄露安全事件时，应当按照学校网络与数据安全事件应急处置预案及时处置并按要求上报。

第二十八条 学校内部若发现违规处理个人信息事件，应当由信息技术中心汇总情况，提交网信领导小组进行初步责任认定，根据发生事件严重程度，移交有关部门依法依纪依规进行处理。

第八章 附则

第二十九条 本办法自公布之日起实施。