广东创新科技职业学院

广创职院〔2021〕141号

广东创新科技职业学院网络信息安全管理规定

第一章　总则

第一条 为了加强广东创新科技职业学院网络信息安全管理，推进信息系统安全等级保护工作，依照《中华人民共和国网络安全法》、《教育部公安部关于全面推进教育行业信息安全等级保护工作的通知》（教技[2015]2 号）等相关法律、制度的要求，制定本管理规定。

第二条 任何单位及个人都必须遵守国家有关法律、法规，不得利用网络危害国家安全、泄露国家秘密，不得侵犯国家、社会、集体利益和个人的合法权益，不得制作、复制、传播和查阅妨碍社会治安、破坏社会稳定，及其他违反宪法和法律、行政法规的不良信息，不得从事违法犯罪活动。

第二章　组织机构与职责

第三条 学校成立网络安全与信息化领导小组，负责学校的网络与信息安全的领导工作，制定各项安全管理制度和整体规划，协调解决安全管理中的重大问题。

第四条 学校党委宣传部是校园网络的信息管理部门，负责学校对外信息发布的审核。学校保卫处负责校园网络信息安全监察和安全事故处理。学校教育技术中心负责校园网信息安全防护与技术保障。

第五条 学校各单位分管信息化工作的领导为本单位网络和信息安全工作的第一责任人，并在单位内指定一名网络信息安全员。该领导和网络信息安全员负责本单位内的网络及信息安全管理工作，按照“谁建设谁负责、谁主管谁监督”的原则对本单位所建设的应用系统、网站、网页等进行管理和检查，若发现有害信息应及时上报并予以删除。

第三章　网络服务安全管理

第六条 所有网络服务的开设需由教育技术中心审批，落实安全责任，完善配套管理制度，做好网络服务备案和信息安全等级保护工作。

第七条 原则上各单位不允许开设 BBS、电子论坛、留言板、聊天室等交互式服务，因特殊原因需开设，要严格办理登记手续，并附有关的管理制度和用户实名注册技术措施，并有专人监控和

管理，对不良信息要及时发现和处理，按公安部门要求保存用户日志，以备追查。

第八条 严格遵守学校校园计算机网络、网站建设及信息系统建设等管理制度中安全方面的规定。

第四章　数据安全管理

第九条 数据的采集和录入要遵循源头、真实、准确、完整、及时的原则。重要数据的录入及修改应指定专人来完成。

第十条 根据数据的保密规定和用途，确定使用人员的存取权限和方式，防止越权操作，禁止私自泄露、外借和转移内部数据与信息。

第十一条 根据学校的职能域将数据进行分类管理。外单位或外部信息系统需要利用或共享数据时，需要书面申请，通过审批后，由学校数据来源部门提供。任何单位和个人不得擅自对外提供学校内部数据。

第十二条 建立数据备份、容灾和恢复机制，加强数据存储和归档管理，确保重要数据有备份、可恢复。

第五章　安全保密管理

第十三条 遵守国家有关法律、法规，严格执行安全保密制

度，不得利用计算机网络进行搜集、整理、窃取、发布或谈论涉及国家及学校机密信息。不得利用电子邮件传递、转发或抄送此类信息。

第十四条 未经审批，学校内部文件、试卷、教案等学校内部信息，以及师生的身份证号、家庭住址和电话等个人隐私信息严禁挂网。

第十五条 发现国家及学校机密泄露的情况，应立即向学校保卫处报告。保卫处按要求上报省教育厅、省公安厅、东莞市公安局、维稳办、派出所等，并配合有关部门查处。

第六章　舆情管理

第十六条 各单位应加强主流舆论的引导，营造出学习先进、弘扬正气的舆论氛围，促成健康、积极的主流舆论的形成。

第十七条 建立网络舆情汇集机制，紧紧围绕师生关注的热点、焦点问题及学校管理决策、师生权益等方面，通过 BBS 论坛、百度贴吧、QQ 群、微信、微博、博客等渠道，进行舆情信息收集，及时掌握苗头性、预警性信息。

第十八条 建立网络舆情分析研判机制，增强舆情危机的预见性。定期组织开展网上信息调研，对采集的舆情信息进行整理分析，准确把握舆情态势，并提出引导舆情或解决问题的对策建议。

第十九条 建立网络舆情干预机制，增强网络舆情可控性。对发现的不良信息，学校第一时间进入应对状态，避免事态扩大。同时，坚持网上网下联动，对师生在网上反映的问题及时落实解决，寓舆情管理于服务之中。

第七章 终端计算机安全管理

第二十条 按照“谁使用，谁负责”的原则，终端计算机使用人负有保管和安全使用的责任。

第二十一条 终端计算机设备上安装、运行的软件须为正版软件。使用盗版软件带来的安全和法律责任由终端计算机使用人承担。

第二十二条 终端计算机使用人应做好数据日常管理和保护，定期进行数据备份。非涉密计算机不得存储和处理涉密信息。

第二十三条 终端计算机使用人应做好终端计算机的安全防范，如发现终端计算机出现可能由病毒或攻击导致的异常系统行为或其他安全问题，应立即断网后进行处理。

第八章 存储介质安全管理

第二十四条 原则上，存储阵列、服务器磁盘等大容量介质应由教育技术中心统一采购和管理，存放在学校数据中心机房。

教育技术中心应采取必要技术措施防范数据泄漏风险，确保存储数据安全。

第二十五条 非涉密移动存储介质不得用于存储涉密信息，不得在涉密计算机上使用。介质使用人应注意存储介质的内容管理，对送出维修或销毁的介质应事先清除敏感信息。介质使用人按照“谁使用，谁负责”的原则，对其移动介质负有保管和安全使用的责任。

第二十六条 涉密介质应当按照秘密载体安全保密要求进行管理。各单位对涉密介质应实行集中管理，责任到人。

第九章 信息安全检查

第二十七条 学校各单位定期对本单位信息系统的安全状况、安全保护制度及措施的落实情况进行自查，并配合教育技术中心的信息安全检查、保密检查等工作。

第二十八条 教育技术中心对学校各单位的信息技术安全工作落实情况进行检查，对发现的问题下达限期整改通知书，责成相关单位制订整改方案并落实到位。

第二十九条 教育技术中心对年度安全检查情况进行全面总结，按照要求完成检查报告并报上级信息安全主管部门。

第十章 信息安全应急管理

第三十条 教育技术中心负责学校信息安全应急工作的统筹管理，负责制定安全事件应急预案，规范网络与信息安全事件报告与处置流程。

第三十一条 学校各单位应按照学校信息安全事件报告与处理流程，做好事件报告与处理工作，做到安全事件早发现、早报告、早控制、早解决。

第三十二条 学校各单位或师生员工均有义务及时向教育技术中心报告网络信息安全事件，不得在未授权情况下对外公布、尝试或利用所发现的安全漏洞或安全问题。

第十二章　安全责任与追究

第三十三条 网络信息安全管理实施“谁使用谁负责、谁主管谁负责”的责任追究制。学校各单位是本单位网络信息安全责任主体，各单位主要负责人为本单位信息安全第一责任人。

第三十四条 对所开设网络服务监管不力造成有害信息传播或秘密信息泄露的单位，给予通报批评和上报学校领导，追究信息安全员责任，情节特别严重的追究单位负责人的领导责任。

第三十五条 各单位或个人收到网络信息安全限期整改通知书后，整改不力或导致严重安全后果的，将根据学校有关规定予以处分。触犯刑律的，移交司法机关处理。

第十三章　附 则

第三十六条 本规定自发文之日起施行。学校原网络信息安全管理规定同时废止。

第三十七条 本规定由教育技术中心负责解释。

广东创新科技职业学院

2021 年 11 月 29 日