校园网网络安全管理制度

一、校园网的安全运行和所有网络设备的管理维护工作由学校信息中心负责。

二、校园网络中心机房要装置调温、调湿、稳压、接地、防雷、防火、防盗等设备，保证网络设备的安全运行，建立完整、规范的校园网设备运行情况档案及网络设备帐目，认真做好各项资料的记录、分类和妥善保存工作。

三、除指定责任人外，其他单位或个人不得以任何方式试图登陆校园网后台管理端，不得对服务器等设备进行修改、设置、删除等操作。

四、校园网对外发布信息的内容，必须经发布信息的学校部门负责人审核并签署意见后，交校办公室审核备案，再由相关责任人予以发布。

五、所有校园网络使用者不得利用各种网络设备或软件技术从事用户账户及口令的侦听、盗用活动，该活动被认为是对校园网网络用户权益的侵犯。

六、为防范黑客攻击，校园网出口处应设置硬件防火墙。若确认已遭到黑客攻击，应尽可能取证，并且信息中心责任人必须在二十四小时内向当地县以上公安机关报告。

七、严禁在校园网上使用来历不明以及可能引发计算机病毒的软件。外来软件应使用经公安部门颁发了《计算机信息系统安全专用产品销售许可证》的杀毒软件检查、杀毒。

八、不得在校园网及其联网计算机上传送危害国家安全的信息(包括多媒体信息)、录阅传送淫秽、色情资料。

九、校园网的系统软件、应用软件及信息数据要实施保密措施。信息资源分不同的保密等级对学校各部门开放。

十、对校园网站内各交互栏目实现管理员24小时巡查制度，双休日、节假日，要有专人检查网络运行情况。

十一、学校网络管理中心必须遵守国家公安部及省公安厅关于网络管理的各项法律、法规和有关技术规范。合理对系统进行安全配置，落实各项网络安全技术防护措施，完善系统定期维护更新措施，落实垃圾邮件、有害信息过滤、封堵技术措施，严格防范病毒、木马、黑客等网络攻击。

十二、服务器系统及各类网络服务系统的系统日志、网络运行日志、用户使用日志等均应严格按照保留60天的要求设置，邮件服务器系统严禁使用匿名转发功能。