**常州市新北区新魏幼儿园网络安全预案**

为及时处置幼儿园信息网络安全事件，保障幼儿园网作用的正常发挥，特制定本预案。

一、幼儿园网络安全事件定义

1、幼儿园网内网站主页被恶意纂改、交互式栏目里发表反政府、分裂国家和色情内容的信息及损害国家、学校声誉的谣言。

2、幼儿园网内网络被非法入侵，应用服务器上的数据被非法拷贝、修改、删除。

3、在网站上发布的内容违反国家的法律法规、侵犯知识版权，已经造成严重后果。

二、网络安全事件应急处理机构及职责

1、设立信息网络安全事件应急处理小组，负责信息网络安全事件的组织指挥和应急处置工作。组长由幼儿园主要负责人担任，成员由分管领导、网络中心等负责人组成。具体承办有关工作组织协调、调查取证、应急处理和对外信息发布等工作。

2、领导机构

幼儿园负责人兼网络安全管理中心组长：丁红波

分管领导兼网络安全管理中心副组长：张留玉

网络安全管理中心组员：冯亚丽、杨昕、任林娟、孙俊洁、朱钰玲

三、网络安全事件报告与处置

事件发生并得到确认后，网络中心或相关科室人员应立即将情况报告有关领导，由领导（组长）决定是否启动该预案，一旦启动该预案，有关人员应及时到位。网络中心在事件发生后24小时内写出事件书面报告。报告应包括以下内容：事件发生时间、地点、单位、事件内容，涉及计算机的IP地址、管理人、操作系统、应用服务，损失，事件性质及发生原因，事件处理情况及采取的措施；事故报告人、报告时间等。网络中心人员进入应急处置工作状态，阻断网络连接，进行现场保护，协助调查取证和系统恢复等工作。对相关事件进行跟踪，密切关注事件动向，协助调查取证。有关违法事件移交公安机关处理。

四、一般性安全隐患处理

学校网络信息中心配备了相应的防火墙软件和瑞星防病毒软件，及时升级，及时清除杀灭网络病毒，检测黑客入侵事件，将向管理员发出警报，管理员将在第一时间处理黑客入侵事件，并报有关部门。对来往电子邮件及网络下载文件用防病毒软件软件过滤，确保不被木马类黑客病毒侵入并在无意中协助传播病毒。

管理员对定期检查设备的运转情况，做好设备维护记录，保证设备高效稳定的运行。一旦主服务出现硬件设备故障，管理员将在第一时间启用备份服务器，保证网络的正常运行，并对原服务器进行及时的检修，在修复后将替换备份服务器继续运行，保证网络的正常运行。凡是上网人员，都能通过防火墙记录在日志里，日志的保留时间为3个月。关闭一些反动、不健康的网站,保障了幼儿园网文化的干净。信息中心对服务器重要信息定时做好备份，提高信息存储安全应急响应能力。并定期检查设备的运转情况，做好设备维护记录，保证设备高效稳定的运行。