八坼中学网络信息发布日常监管与应急预案

为了切实做好学校校园网站、微信公众号信息发布突发事件的防范和应急处理工作，进一步提高学校预防和控制网络突发事件的能力和水平，减轻或消除突发事件的危害和影响，确保校园网络与信息安全，结合学校工作实际，制定本预案。

一、成立安全应急领导小组，明确分工，落实责任。

(一)成立学校网络安全应急领导小组，领导小组成员如下：

组　长：钱志祥

副组长：朱雪兵

组　员：朱小方、李琴、朱巧生、马勤良、褚震雨、沈国民、赵燕

(二)明确领导小组的主要职责:

1.加强领导，健全组织，强化工作职责，完善各项应急预案的制定和各项措施的落实。

2.充分利各种渠道进行网络安全知识的宣传教育，组织、指导全校网络安全常识的普及教育，广泛开展网络安全和有关的技能训练，不断提高广大师生的防范意识和基本技能。

3.认真搞好各项物资保障，严格按照预案要求积极配备网络安全设施设备，落实网络线路、交换设备、网络安全设备等物资，强化管理，使之保持良好的工作状态。

4.采取一切必要手段，组织各方面力量全面进行网络安全事故处理工作，把不良影响与损失降到最低点。

5.调动一切积极因素，全面保证和促进学校网络安全稳定地运

行。

二、各级应急处理预案：

(一)网站不良信息事故处理预案

1.一旦发现学校网站上出现不良信息，立刻关闭网站。

2.备份不良信息出现的目录、出现时间前后一星期的 HTTP 连接日志和网络连接日志。

3.打印不良信息页面留存。

4.完全隔离出现不良信息的目录，使其不能再被访问。

5.删除不良信息，并清查整个网站所有内容，确保没有任何不良信息，重新开通网站服务，并测试网站运行。

6.修改该目录名，对该目录进行安全性检测，升级安全级别，升级程序，去除不安全隐患，关闭不安全栏目，重新开放该目录的网络连接，并进行测试，正常后，重新修改该目录的上级链接。

7.全面排查 HTTP 日志，防火墙网络连接日志，确定不良信息的源 IP 地址，如果来自校内，则立刻全面升级此次事件为最高紧急事件，立刻向领导小组组长汇报，视情节严重程度领导小组可决定是否向公安机关报案。

8.从事故一发生到处理事件的整个过程，必须保持向领导小组组长汇报、解释此次事故的发生情况、发生原因、处理过程。

(二)网络恶意攻击事故处理预案

1.发现网络恶意攻击，立刻确定该攻击来自校内还是校外；受攻击的设备有哪些；影响范围有多大。并迅速推断出此次攻击的最坏结果，

判断是否需要紧急切断校园网的服务器及公网的网络连接，以保护重要数据及信息。

2.如果攻击来自校外，立刻从防火墙中查出对方 IP 地址并过滤，同时对防火墙设置对此类攻击的过滤，并视情况严重程度决定是否报警。

3.如果攻击来自校内，立刻确定攻击源，查出该攻击出自哪台交换机，出自哪台电脑，出自哪位教师或学生。接着立刻赶到现场，关闭该计算机网络连接，并立刻对该计算机进行分析处理，确定攻击出于无意、有意还是被利用。暂时扣留该电脑。

4.重新启动该电脑所连接的网络设备，直至完全恢复网络通信。

5.对该电脑进行分析，清除所有病毒、恶意程序、木马程序以及文件，测试运行该电脑 5 小时以上，并同时进行监控，无问题后归还该电脑。

6.从事故一发生到处理事件的整个过程，必须保持向领导小组组长汇报、解释此次事故的发生情况、发生原因、处理过程。

(三)学校重大网络事件处理预案

1.对学校重大事件进行评估、确定所需要的网络设备及环境。

2.关闭其它与该网络相连、才能对该网络造成不利影响的一切网络设备及计算机，保障该网络的畅通。

3.对重要网络设备提供备份，出现问题需尽快更换设备。

4.对外网连接进行监控，清除非法连接，出现重大问题立刻向上级部门求救。

5.事先应向领导小组汇报本次事件中所需用到的设备、环境、以及可

能出现事故的影响，在事件过程中出现任何问题应立刻向领导小组组长汇报。

三、日常管理

1.领导小组依法发布有关消息和警报，全面组织各项网络安全防御、处理工作。各有关组员随时准备执行应急任务。

2.网络管理员对校园内外所属网络硬件软件设备及接入网络的计算机设备定期进行全面检查，封堵、更新有安全隐患的设备及网络环境。

3.加强对校园网内的计算机设备的管理，加强对学校网络的使用者(学生和教师)的网络安全教育。加强对重要网络设备的软件防护以及硬件防护，确保正常的运行软件硬件环境。

4.加强各类值班值勤，保持通讯畅通，及时掌握学校情况，全力维护正常教学、工作和生活秩序。

5、按预案落实各项物资准备。

四、网络安全事故发生后有关行动

1.领导小组得悉网络紧急情况后立即赶赴本级指挥所，各种网络安全事故处理小组迅速集结待命。

2.应急小组成员听从组织指挥，迅速组织本级抢险防护。

①确保 WEB 网站信息安全为首要任务，迅速发出紧急警报，所有相关成员集中进行事故分析，确定处理方案。

②确保校内其它接入设备的信息安全，经过分析，可以迅速关闭、切断其他接入设备的所有网络连接，防止滋生其他接入设备的安全事故。

③分析网络，确定事故源，使用各种网络管理工具，迅速确定事故源，按相关程序进行处理。

④事故源处理完成后，逐步恢复网络运行，监控事故源是否仍然存在。

⑤针对此次事故，进一步确定相关安全措施、总结经验、加强防范。

⑥从事故一发生到处理的整个过程，必须及时向领导小组组长汇报，听从安排，注意做好保密工作。

3.积极做好广大师生的思想宣传教育工作，迅速恢复正常秩序，全力维护校园网安全稳定。

4.迅速了解和掌握事故情况，及时汇总上报。

5.事后迅速查清事件发生原因，查明责任人，并报领导小组根据责任情况进行处理。

五、其他

1.在应急行动中，学校各部门要密切配合，服从指挥，确保政令畅通和各项工作的落实。

2.各部门应根据本预案，结合本部门实际情况，加强演练与熟悉，切实落实各项组织措施。

苏州市吴江区八坼中学

2021.9