北京师范大学-香港浸会大学联合国际学院
个人信息安全事件应急预案

第一章 总则

第一条 为防范和应对师生个人信息保护突发事件（以下简称突发事件），最大程度地减轻突发事件对师生和学校的损害，保护师生合法权益，保障我校正常经营秩序，根据《中华人民共和国个人信息保护法》等规章制度，结合我校实际制定本预案。

第二条 本预案适用于因信息技术故障、自然灾害或其他突发事件、人为因素造成我校师生个人信息发生泄露、丢失、损坏、篡改或不当使用，损害师生利益，影响我校声誉和正常教学的突发事件。

第三条 工作原则

（一）合法合规原则。突发事件应急处理流程和处置方法必须严格遵守相关法律法规和我校规章制度。

（二）分级管理原则。根据突发事件的特点和影响程度对突发事件分级管理，针对不同等级的突发事件采取不同的应急处理流程。

（三）高效处置原则。对突发事件应快速响应，高效处置，最大限度的化解风险、减少损失。

第二章 突发事件的分级

第四条 突发事件根据性质、影响和危害，划分为特别重大突发事件（Ⅰ级）、重大突发事件（Ⅱ级）和较大突发事件（Ⅲ级）。

事件等级 分级标准	特别重大突发事件（Ⅰ）级	重大突发事件（Ⅱ）级	较大突发事件（Ⅲ）级
影响和危害程度	对师生或我校利益及声誉造成特别重大损害；对我校业务秩序造成特别重大影响。	对师生或我校利益及声誉造成重大损害；对我校业务秩序造成重大影响。	对师生或我校利益及声誉造成较大损害；对我校业务秩序造成较大影响。
信息技术故障	1.两个（含）以上的部门因同一原因丢失、泄露、损毁重要敏感信息。 2.部门丢失、泄露、损毁重要敏感信息1000条（含）以上或师生其他信息5000条（含）以上的。	部门丢失、泄露、损毁重要敏感信息200条（含）以上或师生其他信息1000条（含）以上的。	部门丢失、泄露、损毁师生信息的。
自然灾害或其他突发事件	丢失、泄露、损毁重要敏感信息1000条（含）以上或师生其他信息5000条（含）以上的。	丢失、泄露、损毁重要敏感信息200条（含）以上或师生其他信息1000条（含）以上的。	丢失、泄露、损毁 师生信息的。
人为因素	1.我校员工非法获取、出售、对外提供重要敏感信息50条（含）以上或师生其他信息500	1.我校员工非法获取、出售、对外提供重要敏感信息或师生其他信息的； 2.我校员工因	我校员工因操作不当意外泄露、篡改、不当使用重要敏感信息或师生其他信息的。

	条（含）以上；2.我校员工因操作不当意外泄露、篡改、不当使用重要敏感信息200条（含）以上或师生其他信息1000条（含）以上。	操作不当意外泄露、篡改、不当使用重要敏感信息50条（含）以上或师生其他信息200条（含）以上。	

第五条 当突发事件同时满足多个级别的定级条件时，按最高级别确定事件等级。突发事件随时间推移升级后，按照升级后的级别进行处理。

第三章 组织体系与职责分工

第六条 成立个人信息保护应急领导小组。

应急领导小组是处理突发事件的决策机构，组长由校长兼任，学校办公室、学生事务处、教务处、招生办公室、信息科技服务中心等涉及师生个人信息管理和使用的部门负责人为领导小组成员。应急领导小组设在学校办公室，以上涉及部门各派一名业务骨干作为办公室成员。

第七条 特别重大突发事件（以下简称Ⅰ级事件）的处置由应急领导小组统一指挥；重大突发事件（以下简称Ⅱ级事件）由应急办公室负责处置并向应急领导小组报告；较大突发事件（以下简称Ⅲ级事件）由事发部门直接处置，并将处置结果报应急办公室备案。

第八条 突发事件应急领导小组职责：

（一）审议和批准个人信息保护突发事件应急预案；

（二）领导和指挥Ⅰ级事件的应急处置；

（三）决定Ⅰ级事件的对外报告和公告；

（四）负责其他重要应急处置事项的决策。

第九条 突发事件应急办公室职责：

（一）编制、修订个人信息保护突发事件应急预案；

（二）接收各个部门Ⅰ、Ⅱ级事件的报告；

（三）向应急领导小组报告Ⅰ级事件；按照应急领导小组指令，推动应急方案的落实；收集汇总和报告突发事件处置情况；

（四）组织协调应急办公室成员单位，制定和实施Ⅱ级事件应急处置方案，并向应急领导小组汇报处置结果；

（五）组织、协调学校应急预案的演练；

（六）负责突发事件应急工作资料档案的归集和保管；

（七）应急领导小组交办的其他事项。

第四章 处置措施及流程

第十条 处置措施

应急处置可采用但不限于以下措施：

（一）做好师生沟通安抚工作，正确解答师生疑问，妥善处置师生投诉；

（二）按照规定程序向公众披露相关信息，或通过媒体报道对突发事件，引导社会舆论，妥善处置负面舆情，维护我校声誉；

（三）维护办公场所秩序，保证师生和我校信息、数据安全；

（四）按照规定向监管部门、政府部门以及公安部门报送事件情况；

（五）采取有效措施弥补系统漏洞，恢复系统运行，恢复正常营业秩

序；

（六）补录、修正师生个人信息；

（七）运用法律手段维护师生和我校合法权益；

（八）按照相关规定追究事件当事人和事发部门责任。

第十一条 Ⅰ级事件处置流程

（一）事发部门在第一时间按照程序报告事件情况，直至学校应急办公室，同时进行先期处置。

（二）学校应急办公室收到报告后，立即向应急领导小组组长汇报，并按指示召集应急领导小组会议，通报事件情况。

（三）应急小组成员根据事件情况提出处置意见，经应急领导小组同意后，按照职责分工组织事发部门落实处置方案。

（四）应急办公室全程跟进事件的处置过程，及时向应急领导小组汇报处置进程和事件发展状况，并根据需要再次召集应急领导小组会议。

（五）突发事件处置完毕后，事发部门向应急领导小组提交完整的处置情况报告。

（六）学校应急办公室记录事件处置过程，整理留存相关资料，建立Ⅰ级突发事件档案。

第十二条 Ⅱ级事件处置流程

（一）事发部门在第一时间按照程序报告事件情况，直至学校应急办公室，同时进行先期处置。

（二）学校应急办公室收到报告后，立即召集应急办公室成员召开应急处理会议，通报事件情况。

（三）应急办公室成员根据事件情况提出处置意见，经讨论通过后，按照职责分工组织事发部门落实处置方案。

（四）应急办公室全程跟进事件的处置过程，及时向应急办公室成员通报处置进程和事件发展状况，并根据需要再次召开应急办公室成员会议。

（五）突发事件处置完毕后，事发部门向应急办公室提交完整的处置情况报告。

（六）学校应急办公室记录事件处置过程，整理留存相关资料，建立Ⅱ级突发事件档案。

第十三条 Ⅲ级事件处置流程

（一）事发部门在第一时间按照程序报告事件情况，同时进行先期处置。

（二）事发部门视事件程度及处理涉及部门情况，按照既定程序，采取有效措施进行处置。处置完毕后，将事件情况和处置方法和结果报学校应急办公室备案。

（三）学校应急办公室审核备案资料，建立Ⅲ级突发事件档案。

第十四条 总结与整改

事发部门应深入分析事件成因，采取有效措施弥补管理、制度、流程和系统上的漏洞，完善预警机制和监督检查措施，杜绝类似事件发生。参与事件处置的部门应对处置过程中进行总结，汲取教训，积累经验，不断提升突发事件反应速度，提高应对措施的针对性和有效性。

第七章 培训与演练

第十五条 宣传与培训

学校各部门要加强对师生个人信息保护知识及应急预案的宣传和培训，提升全校师生个人信息保护意识和突发事件的应急处理能力。

第十六条 应急演练

学校每两年开展一次师生个人信息突发事件应急演练。演练由学校应急办公室负责组织，各相关业务部门提供演练案例，并按照演练方案完成演练工作。学校根据自身情况和当地监管要求确定演练频率，原则上不低于两年一次。应急演练方案、演练的组织实施等应形成档案长期留存。