# 最新校园网络安全管理制度汇编 校园网络安全管理制度 微博(十四篇)

来源：网络 作者：明月清风 更新时间：2024-08-21

*人的记忆力会随着岁月的流逝而衰退，写作可以弥补记忆的不足，将曾经的人生经历和感悟记录下来，也便于保存一份美好的回忆。相信许多人会觉得范文很难写？接下来小编就给大家介绍一下优秀的范文该怎么写，我们一起来看一看吧。校园网络安全管理制度汇编 校园...*

人的记忆力会随着岁月的流逝而衰退，写作可以弥补记忆的不足，将曾经的人生经历和感悟记录下来，也便于保存一份美好的回忆。相信许多人会觉得范文很难写？接下来小编就给大家介绍一下优秀的范文该怎么写，我们一起来看一看吧。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇一**

二、网络管理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，要建立完整、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(软件)的记录、分类和妥善保存工作。

三、除网络管理中心外，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web服务器中的内容，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，由网络管理中心从技术上开通其对外的信息服务。

五、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。若遭到黑客攻击，网络管理中心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。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇二**

为了加强领导，完善管理，建立严密的网络安全人员组织机制，我校特成立网络安全领导小组，领导小组日常基本工作要求如下：

1、提高认识，从讲政治的高度认识网络安全的重要性。

2、积极采取措施杜绝他人利用校园网从事危害国家安全、泄露国家机密、违法犯罪等活动。

3、制定、落实计算机系统安全操作规程，并定期检讨和更新，保证适应新时期的要求、可执行性强。

4、组织相关规章制度、法律法规知识的学习，加强计算机法制宣传活动。

5、设立专门人员对计算机网络、设备统一规划和管理，做到设备不乱用、专职专人专责，落实各级责任人、工作任务清晰、责任到位。

6、每天必须进行系统巡查，包括检查网站、论坛、留言板（bbs）等栏目内容，落实信息先审后发制度，及时发现问题。

7、每次系统变更（新增、减少、更改配置等）应做好备案登记，每周进行一次系统清点，对新变动的系统部分及时跟踪。

8、每周对操作系统、防病毒系统进行升级、打补丁。

9、加强密码设置和保护，设置复杂密码，经常修改密码。经常进行数据备份。

10、积极配合上级部门的计算机系统安全保障工作，积极了解最新的安全技术发展动态和规定。

11、发现网络异常、系统遭到恶意攻击和破坏、内容被删改、或者出现不良、反动等信息迹象，不得马上修复系统资料和数据，应先立即保护好现场，备份案件记录和历史数据，同时及时上报区教育网络中心。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇三**

学校校园网是为教学及学校管理而建立的计算机信息网络，目的在于利用先进实用的计算机技术和网络通信技术，实现校园内计算机互联、资源共享，并为师生提供丰富的网上资源。为了保护校园网络系统的安全、促进学校计算机网络的应用和发展，保证校园网络的正常运行和网络用户的使用权益，更好的为教育教学服务，特制定如下管理条例。

1、本管理制度所称的校园网络系统，是指由校园网络设备、配套的网络线缆设施、网络服务器、工作站所构成的，为校园网络应用而服务的硬件、软件的集成系统。

2、校园网络的安全管理，应当保障计算机网络设备和配套设施的安全，保障信息的安全和运行环境的安全，保障网络系统的正常运行，保障信息系统的安全运行。

3、我校成立了网络安全领导小组，组长由学校法人担任，从事校园网络管理的人员要具有相应的法律意识和计算机网络管理水平，必须成立校园网络安全管理机构，负责校园内的网络安全和信息安全工作，定期对相应的网络用户进行有关信息安全和网络安全教育并对上网信息进行审查和监控。

4、任何单位和个人，未经学校法人或校园网络中心同意，不得擅自安装、拆卸或改变网络设备。

5、所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。任何单位和个人不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动。

6、进入校园网的全体学生、教职员工必须接受并配合国家有关部门及学校依法进行的监督检查，必须接受学校网络中心进行的网络系统及信息系统的安全检查。

7、使用校园网的全体师生有义务向学校法人、网络中心和有关部门报告违法行为和有害信息。

1、校园网由学校统一管理及维护。接入校园网的各部门、处室、教室和个人使用者必须严格使用自己的用户名和密码上网。网络管理员对入网计算机和使用者进行登记，由网络中心负责对其进行监督和检查。任何人不得更改ip及网络设置，不得盗用用户帐号。

2、与校园网相连的计算机用户建设应当符合国家的有关标准和规定，校园内从事施工、建设，不得危害计算机网络系统的安全。

3、网络管理员负责全校网络及信息的安全工作，要及时解决突发事件和问题。校园网各服务器发生案件、以及遭到黑客攻击后，网络中心必须及时备案并向公安机关报告。

4、对所有联网计算机要及时、准确登记备案。网络教室未经允许不准对社会开放。

5、校园网中对外发布信息的web服务器中的内容必须经领导审核，由负责人审核通过后再进行发布。新闻公布、公文发布权限要经过对应部门领导的批准。对网站内容要进行定期更新、备份。

6、校园网各类服务器中开设的帐户和口令为个人用户所拥有，网络中心对用户口令保密，不得向任何单位和个人提供这些信息。校园网及子网的系统软件、应用软件及信息数据要实施保密措施。

7、加强对师生用户上网安全教育指导和监督：

（1）校园网内必须安装网络版监控和防范不良信息的过滤软件系统，监控日志同时上报县教育局电教室。

（2）加强对学生开放互联网以及全校教职工上网的监管。

（3）专用的财务工作电脑和重要管理数据的电脑最好不要接入网络工作。

8、校园网络内的每台计算机上必须安装防病毒软件，各部门、教研组、办公室要切实做好防病毒措施，随时注意杀毒软件是否开启，及时在线升级杀毒软件，及时向网络中心报告陌生、可疑邮件和计算机非正常运行等情况。

9、禁止私自安装、卸载程序，在校园网上，禁止使用盗版软件，不允许玩网络游戏，不允许无关人员使用，也不允许进行与工作无关的操作，禁止任意修改和删除计算机的系统文件和系统设置。

10、严禁在校园网内使用来历不明、引发病毒传染的软件或文件；对于外来光盘、优盘上的文件应使用合格的杀毒软件进行检查、杀毒。

11、任何单位和个人不得在校园网及其连网计算机上录阅传送有政治问题和淫秽色情内容的信息。

12、未经校园网络中心及各子网网管的同意，不得将有关服务器、工作站上的系统软件、应用软件转录、传递到校外。

13、需在校内交流和存档的数据，按规定地址存放，不得存放在硬盘的c盘区，私人文件不得保存在工作电脑中，由此造成的文件丢失损坏等后果自负。

14、保护校园网的设备和线路，不准擅自改动计算机的连接线，不准打开计算机主机的机箱，不准擅自移动计算机、线路设备及附属设备，不准擅自把计算机设备外借。

15、各处室部门和教研组必须加强对计算机的管理，指定专人负责管理。管理员应经常测试计算机设备的性能，发现故障及时通过校园办公系统上报。

16、各处室部门和教研组应认真做好本单位计算机的维护和清洁卫生工作。

1、使用校园网的全体师生必须对所提供的信息负责。严禁制造和输入计算机病毒，以及其他有害数据，危害计算机信息系统的安全，不得利用计算机联网从事危害家安全、泄露秘密等犯罪活动，不得制作、查阅、复制和传播有敏感信息和有害信息。

2、除校园网负责人员外，其他单位或个人不得以任何方式试图登陆进入校园网服务器或计算机等设备进行修改、设置、删除等操作；任何单位和个人不得以任何借口盗窃、破坏网络设施。

3、用户要严格遵守校园网络管理规定和网络用户行为规范，不随意把户名借给他人使用，增强自我保护意识，经常更换口令，保护好用户名和密码。严禁用各种手段解决他人口令、盗用户名和密码。

4、网络用户不得利用各种网络设备或软件技术从事用户帐户及口令的侦听、盗用活动。

5、使用校园网的全体师生有义务向网络中心报告违法行为和有害的、不健康的信息。

违反本制度规定，有下列行为之一的，学校可根据情节提出警告、停止其上网，情节严重者给予行政处分，或交公安机关处理。

1、查阅、复制或传播下列信息

（1）煽动分裂国家、破坏国家统一和民族团结、推翻社会主义制度；

（2）煽动抗拒、破坏宪法和国家法律、行政法规的实施；

（3）捏造或者歪曲事实，故意散布谣言，扰乱社会秩序；

（4）公然侮辱他人或者捏造事实诽谤他人；

（5）宣扬封建迷信、淫秽、色情、暴力、凶杀、恐怖等。

2、破坏、盗用计算机网络中的信息资源和进行危害计算机网络安全的活动。

3、盗用他人帐号或私自转借、转让用户帐号造成危害者；

4、故意制作、传播计算机病毒等破坏性程序者。

5、上网信息审查不严，造成严重后果者。

6、使用任何工具破坏网络正常运行或窃取他人信息者。

7、有盗用用户名和口令、解决用户口令等危及网络安全运行与管理的恶劣行径者。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇四**

智慧校园校园网是为教学工作及学校管理而建立的计算机信息网络，目的在于利用先进实用的计算机技术和网络通信技术，实现校园内计算机互联、资源共享，并为师生提供丰富的网上资源。为了保护校园网络系统的安全、促进学校计算机网络的应用和发展，保证校园网络的正常运行和网络用户的使用权益，更好的为教育教学服务，特制定如下管理制度。

一、本管理制度所称的校园网络系统，是指由校园网络设备、配套的网络线缆设施、网络服务器、工作站所构成的，为校园网络应用而服务的硬件、软件的集成系统。

二、校园网络的安全管理，应当保障计算机网络设备和配套设施的安全，保障信息的安全和运行环境的安全，保障网络系统的正常运行，保障信息系统的安全运行。

三、校园网实行统一管理、分级负责制。网络中心负责对校园网资源进行管理，负责全校的网络安全和信息安全工作，定期对相应的网络用户进行有关信息安全和网络安全教育并对上网信息进行审查和监控；各处室及办公室负责对本部门资源进行管理；各部门计算机责任人负责对本部门计算机系统的管理。有关校园网上进行学校信息发布、新闻宣传系统、管理信息系统等方面的信息服务，归口学校办公室负责。

四、任何单位和个人，未经校园网网络中心同意，不得擅自安装、拆卸或改变网络设备。

五、所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。任何单位和个人不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动。

六、进入校园网的全体学生、教职员工必须接受并配合国家有关部门及学校依法进行的监督检查，必须接受学校网络中心进行的网络系统及信息系统的安全检查。

七、使用校园网的全体师生有义务向网络中心和有关部门报告违法行为和有害信息。

一、校园网由学校网络中心统一管理及维护。连入校园网的各部门、处室、教室和个人使用者必须严格使用由网络中心分配的ip地址。网络管理员对入网计算机和使用者进行登记，由网络中心负责对其进行监督和检查。任何人不得更改ip及网络设置，不得盗用ip地址及用户帐号。

二、与校园网相连的计算机用户建设应当符合国家的有关标准和规定，校园内从事施工、建设，不得危害计算机网络系统的安全。

三、网络管理员负责全校网络及信息的安全工作，建立网络事故报告并定期汇报，及时解决突发事件和问题。校园网各服务器发生案件、以及遭到黑客攻击后，网络中心必须及时备案并向公安机关报告。

四、对所有联网计算机要及时、准确登记备案。网络教室不准对社会开放。

五、校园网中对外发布信息的web服务器中的内容必须经领导审核，由负责人签署意见后再由信息员发布。新闻公布、公文发布权限要经过校领导的批准。

六、校园网各类服务器中开设的帐户和口令为个人用户所拥有，网络中心对用户口令保密，不得向任何单位和个人提供这些信息。校园网及子网的系统软件、应用软件及信息数据要实施保密措施。

七、加强对师生用户上网安全教育指导和监督：

1、校园网内必须安装网络版监控和防范不良信息的过滤软件系统，监控日志至少保存半年。

2、加强对学生开放互联网以及全校教职工上网的监管。

3、专用的财务工作电脑和重要管理数据的电脑最好不要接入网络工作。

八、网络中心统一在每台计算机上安装防病毒软件，各部门、教研组、办公室要切实做好防病毒措施，随时注意杀毒软件是否开启，及时在线升级杀毒软件，及时向网络中心报告陌生、可疑邮件和计算机非正常运行等情况。

九、禁止私自安装、卸载程序；在校园网上，禁止使用盗版软件，不允许玩计算机游戏，不允许无关人员使用，也不允许进行与工作无关的操作，禁止任意修改和删除计算机的系统文件和系统设置。

十、严禁在校园网内使用来历不明、引发病毒传染的软件或文件；对于外来光盘、优盘、软盘上的文件应使用合格的杀毒软件进行检查、消毒。

十一、任何单位和个人不得在校园网及其连网计算机上录阅传送有政治问题和淫秽色情内容的信息。

十二、未经校园网络中心及各子网网管的同意，不得将有关服务器、工作站上的系统软件、应用软件转录、传递到校外。

十三、需在校内交流和存档的数据，按规定地址存放，不得存放在硬盘的c盘区，私人文件不得保存在工作电脑中，由此造成的文件丢失损坏等后果自负。

十四、保护校园网的设备和线路，不准擅自改动计算机的连接线，不准打开计算机主机的机箱，不准擅自移动计算机、线路设备及附属设备，不准擅自把计算机设备外借。

十五、各处室部门和教研组必须加强对计算机的管理，指定专人负责管理。管理员应经常测试计算机设备的性能，发现故障及时通知网络中心处理。

十六、各处室部门和教研组应认真做好本单位计算机的养护和清洁卫生工作。

一、使用校园网的全体师生必须对所提供的信息负责。严禁制造和输入计算机病毒，以及其他有害数据，危害计算机信息系统的安全，不得利用计算机联网从事危害国家安全、泄露秘密等犯罪活动，不得制作、查阅、复制和传播有碍社会治安和有伤风化的信息。

二、除校园网负责人员外，其他单位或个人不得以任何方式试图登陆进入校园网服务器或计算机等设备进行修改、设置、删除等操作；任何单位和个人不得以任何借口盗窃、破坏网络设施，这些行为被视为对校园网安全运行的破坏行为。

三、用户要严格遵守校园网络管理规定和网络用户行为规范，不随意把帐号借给他人使用，增强自我保护意识，经常更换口令，保护好帐号和ip地址。严禁用各种手段破解他人口令、盗用帐号和ip地址。

四、网络用户不得利用各种网络设备或软件技术从事用户帐户及口令的侦听、盗用活动，该活动被认为是对网络用户权益的侵犯。

五、使用校园网的全体师生有义务向网络中心报告违法行为和有害的、不健康的信息。

违反本制度规定，有下列行为之一者，学校可提出警告、停止其上网，情节严重者给予行政处分，或提交司法部门处理。

一、查阅、复制或传播下列信息者：

1、煽动分裂国家、破坏国家统一和民族团结、推翻社会主义制度。

2、煽动抗拒、破坏宪法和国家法律、行政法规的实施。

3、捏造或者歪曲事实，故意散布谣言，扰乱社会秩序。

4、公然侮辱他人或者捏造事实诽谤他人。

5、宣扬封建迷信、淫秽、色情、暴力、凶杀、恐怖等。

二、破坏、盗用计算机网络中的信息资源和进行危害计算机网络安全的活动。

三、盗用他人帐号或私自转借、转让用户帐号造成危害者。

四、故意制作、传播计算机病毒等破坏性程序者。

五、上网信息审查不严，造成严重后果者。

六、使用任何工具破坏网络正常运行或窃取他人信息者。

七、有盗用ip地址、盗用帐号和口令、破解用户口令等危及网络安全运行与管理的恶劣行径者。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇五**

学校校园网是为教学及学校管理而建立的计算机信息网络，目的在于利用先进实用的计算机技术和网络通信技术，实现校园内计算机互联、资源共享，并为师生提供丰富的网上资源。为了保护校园网络系统的安全、促进学校计算机网络的应用和发展，保证校园网络的正常运行和网络用户的使用权益，更好的为教育教学服务，特制定如下管理条例。

1、本管理制度所称的校园网络系统，是指由校园网络设备、配套的网络线缆设施、网络服务器、工作站所构成的，为校园网络应用而服务的硬件、软件的集成系统。

2、校园网络的安全管理，应当保障计算机网络设备和配套设施的安全，保障信息的安全和运行环境的安全，保障网络系统的正常运行，保障信息系统的安全运行。

3、网络中心负责相应的网络安全和信息安全工作，定期对相应的网络用户进行有关信息安全和网络安全教育并对上网信息进行审查和监控。

4、任何单位和个人，未经校园网网络中心同意，不得擅自安装、拆卸或改变网络设备。

5、所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。任何单位和个人不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动。

6、进入校园网的全体学生、教职员工必须接受并配合国家有关部门及学校依法进行的监督检查，必须接受学校网络中心进行的网络系统及信息系统的安全检查。

7、使用校园网的全体师生有义务向网络中心和有关部门报告违法行为和有害信息。

1、校园网由学校电教中心统一管理及维护。连入校园网的各部门、处室、教室和个人使用者必须严格使用由网络中心分配的ip地址。网络管理员对入网计算机和使用者进行登记，由网络中心负责对其进行监督和检查。任何人不得更改ip及网络设置，不得盗用ip地址及用户帐号。

2、与校园网相连的计算机用户建设应当符合国家的有关标准和规定，校园内从事施工、建设，不得危害计算机网络系统的安全。

3、网络管理员负责全校网络及信息的安全工作，建立网络事故报告并定期汇报，及时解决突发事件和问题。校园网各服务器发生案件、以及遭到黑客攻击后，网络中心必须及时备案并向公安机关报告。

4、对所有联网计算机要及时、准确登记备案。网络教室不准对社会开放。

5、校园网中对外发布信息的web服务器中的内容必须经领导审核，由负责人签署意见后再由信息员发布。新闻公布、公文发布权限要经过校领导的批准。

6、校园网各类服务器中开设的帐户和口令为个人用户所拥有，网络中心对用户口令保密，不得向任何单位和个人提供这些信息。校园网及子网的系统软件、应用软件及信息数据要实施保密措施。

7、加强对师生用户上网安全教育指导和监督：

（1）校园网内必须安装网络版监控和防范不良信息的过滤软件系统，监控日志至少保存半年。

（2）加强对学生开放互联网以及全校教职工上网的监管。

（3）专用的财务工作电脑和重要管理数据的电脑最好不要接入网络工作。

8、网络中心统一在每台计算机上安装防病毒软件，各部门、教研组、办公室要切实做好防病毒措施，随时注意杀毒软件是否开启，及时在线升级杀毒软件，及时向网络中心报告陌生、可疑邮件和计算机非正常运行等情况。

9、禁止私自安装、卸载程序，在校园网上，禁止使用盗版软件，不允许玩电子游戏，不允许无关人员使用，也不允许进行与工作无关的操作，禁止任意修改和删除计算机的系统文件和系统设置。

10、严禁在校园网内使用来历不明、引发病毒传染的软件或文件；对于外来光盘、优盘、软盘上的文件应使用合格的杀毒软件进行检查、消毒。

11、任何单位和个人不得在校园网及其连网计算机上录阅传送有政治问题和淫秽色情内容的信息。

12、未经校园网络中心及各子网网管的同意，不得将有关服务器、工作站上的系统软件、应用软件转录、传递到校外。

13、需在校内交流和存档的数据，按规定地址存放，不得存放在硬盘的c盘区，私人文件不得保存在工作电脑中，由此造成的文件丢失损坏等后果自负。

14、保护校园网的设备和线路，不准擅自改动计算机的连接线，不准打开计算机主机的机箱，不准擅自移动计算机、线路设备及附属设备，不准擅自把计算机设备外借。

15、各处室部门和教研组必须加强对计算机的管理，指定专人负责管理。管理员应经常测试计算机设备的性能，发现故障及时通知网络中心处理。

16、各处室部门和教研组应认真做好本单位计算机的养护和清洁卫生工作。

1、使用校园网的全体师生必须对所提供的信息负责。严禁制造和输入计算机病毒，以及其他有害数据，危害计算机信息系统的安全，不得利用计算机联网从事危害家安全、泄露秘密等犯罪活动，不得制作、查阅、复制和传播有碍社会治安和有伤风化的信息。

2、除校园网负责人员外，其他单位或个人不得以任何方式试图登陆进入校园网服务器或计算机等设备进行修改、设置、删除等操作；任何单位和个人不得以任何借口盗窃、破坏网络设施，这些行为被视为对校园网安全运行的破坏行为。

3、用户要严格遵守校园网络管理规定和网络用户行为规范，不随意把户头借给他人使用，增强自我保护意识，经常更换口令，保护好户头和ip地址。严禁用各种手段破解他人口令、盗用户头和ip地址。

4、网络用户不得利用各种网络设备或软件技术从事用户帐户及口令的侦听、盗用活动，该活动被认为是对网络用户权益的侵犯。

5、使用校园网的全体师生有义务向网络中心报告违法行为和有害的、不健康的信息。

违反本制度规定，有下列行为之一者，学校可提出警告、停止其上网，情节严重者给予行政处分，或提交司法部门处理。

1、查阅、复制或传播下列信息者：

（1）煽动分裂国家、破坏国家统一和民族团结、推翻社会主义制度；

（2）煽动抗拒、破坏宪法和国家法律、行政法规的实施；

（3）捏造或者歪曲事实，故意散布谣言，扰乱社会秩序；

（4）公然侮辱他人或者捏造事实诽谤他人；

（5）宣扬封建迷信、淫秽、色情、暴力、凶杀、恐怖等。

2、破坏、盗用计算机网络中的信息资源和进行危害计算机网络安全的活动。

3、盗用他人帐号或私自转借、转让用户帐号造成危害者；

4、故意制作、传播计算机病毒等破坏性程序者。

5、上网信息审查不严，造成严重后果者。

6、使用任何工具破坏网络正常运行或窃取他人信息者。

7、有盗用ip地址、盗用帐号和口令、破解用户口令等危及网络安全运行与管理的恶劣行径者。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇六**

1、学校成立网络管理领导小组和网络维护小组。维护小组由管理员和信息技术教师组成，负责在网络管理领导小组指导下进行日常维护。

2、网络用户是指使用网络的各部门及个人。

3、学校鼓励各部门、各科室、各学科组和全体师生使用网络资源。

4、网络维护小组根据教育网信息管理中心要求为每科室、学科组、个人统一分配ip地址，其他人不得随意更改，如有需要报维护小组进行修改。

5、各科室、学科组和个人在使用网络过程中必须遵守国家有关法律、法规和信息中心的有关规定。

6、用户在使用网络时违反国家法律和行政法规的，学校将视情节轻重给予警告、通报批评，情节特别严重构成犯罪的，报有关部门依法追究刑事责任。

7、禁止各用户上不良网站。通过聊天、邮件而传播网络病毒的，维护小组要及时提醒，要求该用户改正，如果是故意行为，将报学校网络管理领导小组进行严肃处理。

8、网络的主干通信设备、主干网络线路、服务器、网络交换机及其它公共设备由维护小组负责管理维护。

9、维护小组对各用户计算机进行对入网设备、安装的软件实行规范管理，不定期进行检查。对安装不健康内容、危害网络安全和一些游戏软件进行及时清除

10、网络信息是指通过网络发布、传递及存储在网络设备中的信息。学校鼓励教师使用网络上有用资源。

11、任何人不得利用学校网络提供的各种信息服务从事危害国家安全、泄露国家机密等犯罪活动，不得制作、查阅、复制和传播危害国家安全、妨碍社会治安和淫秽色情的信息。

12、发生重大突发事件期间，学校网络安全管理领导小组要加强网络监控，及时、果断地处置网上突发事件。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇七**

第一条所有接入网络的用户必须遵守国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。任何单位和个人不得利用连网计算机从事危害城域网及校园网防火墙、路由器、交换机、服务器等网络设备的活动。不得在网络上制作、发布、传播下列有害内容：

（一）泄露国家秘密，危害国家安全的；

（二）违反国家民族、宗教与教育政策的；

（三）煽动暴力，宣扬封建迷信、邪教、黄色淫秽，违反社会公德，以及赌博、诈骗和教唆犯罪的；

（四）公然侮辱他人或者捏造事实诽谤他人的，暴露个人隐私和攻击他人与损害他人合法权益的；

（五）散布谣言，扰乱社会秩序，鼓励聚众滋事的；

（六）损害社会公共利益的；

（七）计算机病毒；

（八）法律和法规禁止的其他有害信息。

如发现上述有害信息内容，应及时向三门县教育局现代教育中心或上级主管部门报告，并采取有效措施制止其扩散。

第二条在网站上发现大量有害信息，以及遭到黑客攻击后，必须在12小时内向三门县教育局现代教育中心及公安机关报告，并协助查处。在保留有关上网信息和日志记录的前题下，及时删除有关信息。问题严重、情况紧急时，应关闭交换机或相关服务器。

第三条任何单位和个人不得在校园网及其连网的计算机上收阅下载传递有政治问题和淫秽色情内容的信息。

第四条所有接入网络的用户必须对提供的信息负责，网络上信息、资源、软件等的使用应遵守知识产权的有关法律法规。对于运行无合法版权的网络软件而引起的版权纠纷由使用部门（个人）承担全部责任。

第五条严禁在网络上使用来历不明、引发病毒传染的软件，对于来历不明的可能引发计算机病毒的软件应使用公安部门推荐的杀毒软件检查、杀毒。

第六条认真执行各项管理制度和技术规范，监控、封堵、清除网上有害信息。为有效地防范网上非法活动、各子网站要加强出口管理和用户管理。重要网络设备必须保持日志记录，时间不少于180天。

第七条上网信息管理坚持“谁上网谁负责、谁发布谁负责”的原则。对外发布信息，必须经局机关或各单位负责人审核批准后，才可发布。

第八条各单位和学校要确定一名行政人员为本单位（学校）网络安全责任人，领导网管员（网管机构）做好本单位和学校的网络和信息安全工作。建立岗位责任制和机房管理制度。网络管理人员应加强责任心，保证现有各种网络设备良好运行，充分发挥效率。

第九条单位和学校各信息终端用户必须受网络管理员监督管理。整个单位和校园要统一出口、统一用户管理。建立帐号登记管理制度，用户帐号只能专人专用，方便日后的检查和监督工作。

第十条与城域网及单位和学校网络相连的机房建设，应当符合国家的有关标准和规定，在电源防护、防盗、防火、防水、防尘、防雷等方面，采取规范的技术保护措施。

第十一条城域网及校园网站的系统软件、应用软件及信息数据要实施保密措施。接入互联网网的计算机必须与本部门的涉密计算机信息系统实行物理隔离。涉密信息不得在上网设备上操作或存储。信息资源保密等级可分为：

（一）可向internet公开的；

（二）可向本城域网公开的；

（三）可向有关单位或个人公开的；

（四）可向本单位公开的；

（五）仅限于个人使用的。

第十二条任何单位和个人不得利用联网计算机从事下列活动：

（一）未经允许，非法访问教育城域网及校园网上网络服务器、工作站、交换机、路由器及其它相关设备；对教育城域网上所具有的功能、程序、数据进行删除、修改和增加；

（二）未经允许，擅自提供与教育无关的网络服务；

（三）故意制作、传播计算机病毒与破坏性程序；

（四）其他危害教育城域网络安全的行为。

第十三条违反本管理制度，将提请有关部门视情节给予相应的批评教育、通报批评或行政处分、处以警告或停机整顿。触犯国家有关法律、行政法规的，依照有关法律、行政法规的规定予以处罚；构成犯罪的，依法追究刑事责任。

第十四条故意输入计算机病毒，造成危害城域网及子网站网络安全的，按《中华人民共和国计算机信息系统安全保护条例》中第二十三条的规定予以处罚。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇八**

1、具体负责校园网网络安全的管理，协调各部门实施校园网网络安全的有关管理措施。

2、维护和管理学院网络版杀毒软件，监控网络病毒，并对用户的网络版杀毒软件使用提供技术支持。

3、负责校园网网络安全的管理，做好各服务器的防病毒和防篡改工作，对服务器进行定期查毒、杀毒，及时下载并安装系统漏洞补丁，采取各种有效措施防止黑客攻击和破坏。

4、对网络的系统及环境进行安全维护，随时监督网络情况，防止黑客入侵、病毒侵害及网络安全，配合有关部门进行相应管理。

5、网络安全人员要协助信息管理中心技术人员定期检查有关网络和服务器系统的运行日志，定期和不定期地进行对全校校园网进行网络安全检查。

6、对校园网上的信息进行管理，随时更新并查看\_信息内容，删除、屏蔽有害信息，为用户提供内容丰富健康的信息服务。

7、定期检查有关网络和服务器系统的运行日志，定期和不定期对校园网进行安全检查。

8、负责与省公安厅、市公安局等有关计算机安全监察部门的联系及有关材料的组织、汇总和上报工作。

9、网络安全员根据国家、地方和学校的有关文件精神，根据校园网的工作需要，提出并组织制定和修订校园网的有关网络安全管理的各项规定并监督实施。

10、网络安全员须积极配合公安等安全和保密的有关执法部门，对网络违法案件进行调查和取证等工作。

11、做好校园网及学校各计算机的安全涉密工作。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇九**

学校校园网是为教学及学校管理而建立的计算机信息网络，目的在于利用先进实用的计算机技术和网络通信技术，实现校园内计算机互联、资源共享，并为师生提供丰富的网上资源。为了保护校园网络系统的安全、促进学校计算机网络的应用和发展，保证校园网络的正常运行和网络用户的使用权益，更好的为教育教学服务，特制定如下管理条例。

1、本管理制度所称的校园网络系统，是指由校园网络设备、配套的网络线缆设施、网络服务器、工作站所构成的，为校园网络应用而服务的硬件、软件的集成系统。

2、校园网络的安全管理，应当保障计算机网络设备和配套设施的安全，保障信息的安全和运行环境的安全，保障网络系统的正常运行，保障信息系统的安全运行。

3、教技领导小组下的网络管理组负责相应的网络安全和信息安全工作，定期对相应的网络用户进行有关信息安全和网络安全教育并对上网信息进行审查和监控。

4、任何单位和个人，未经管理组同意，不得擅自安装、拆卸或改变网络设备。

5、所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。任何单位和个人不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动。

6、进入校园网的全体学生、教职员工必须接受并配合国家有关部门及学校依法进行的监督检查，必须接受学校网络管理组进行的网络系统及信息系统的安全检查。

7、使用校园网的全体师生有义务向网络管理组和有关部门报告违法行为和有害信息。

1、校园网由学校网络管理小组统一管理及维护。连入校园网的各部门、教室和个人使用者必须严格使用由网络中心分配的ip地址。网络管理员对入网计算机和使用者进行登记，由网络中心负责对其进行监督和检查。任何人不得更改ip及网络设置，不得盗用ip地址及用户帐号。

2、与校园网相连的计算机用户建设应当符合国家的有关标准和规定，校园内从事施工、建设，不得危害计算机网络系统的安全。

3、网络管理员负责全校网络及信息的安全工作，建立网络事故报告制度并定期汇报，及时解决突发事件和问题。校园网各服务器发生案件、以及遭到黑客攻击后，网络管理组必须及时备案并向公安机关报告。

4、对所有联网计算机要及时、准确登记备案。校园网络不准对社会开放。

5、校园网中对外发布信息的web服务器中的内容必须经领导审核，由负责人签署意见后再由信息员发布。新闻公布、公文发布权限要经过校领导的批准。

6、校园网各类服务器中开设的帐户和口令为个人用户所拥有，网络管理组对用户口令保密，不得向任何单位和个人提供这些信息。校园网及子网的系统软件、应用软件及信息数据要实施保密措施。

7、加强对师生用户上网安全教育指导和监督：

（1）校园网内必须安装网络版监控和防范不良信息的过滤软件系统，监控日志至少保存半年。

（2）加强对学生开放互联网以及全校教职工上网的监管。

（3）专用的财务工作电脑和重要管理数据的电脑最好不要接入网络工作。

8、网络管理小组统一在每台计算机上安装防病毒软件，各部门、教研组、办公室要切实做好防病毒措施，随时注意杀毒软件是否开启，及时在线升级杀毒软件，及时向网络管理组报告陌生、可疑邮件和计算机非正常运行等情况。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇十**

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网络管理中心负责。

二、网络管理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，要建立完整、规范的校园网设备运行情况档案及网络设备账目，认真做好各项资料（软件）的记录、分类和妥善保存工作。

三、除网络管理中心外，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web服务器中的内容，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，由网络管理中心从技术上开通其对外的信息服务。

五、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。若遭到黑客攻击，网络管理中心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、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，监控、封堵、清除网上有害信息。为了有效地防范网上非法活动，校园网要统一出口管理、统一用户管理，进出校园网访问信息的所有用户必须使用网络管理中心负责设立的代理服务器、email服务器。

十二、服务器必须保持日志记录功能，历史记录保持时间不得低于2个月。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇十一**

一、校园网络设施系学校贵重财产和精密设备，学校师生应严格执行有关规定。

二、校园网络要有完备的防火、防潮、防盗、防磁、防雷、防触电、防病毒和防黑客侵入等设备和措施。中心机房应安装空调，保持室温、温度稳定。

三、学校应制定《网络事故安全预案》，全校师生应掌握其相关内容。当发生紧急事件时按照《网络事故安全预案》进行处理。

四、校园网络管理人员负责监控校园网络的运行状态，随时了解网络运行情况，如有异常，应及时处理，保证学校的教育教学和各项管理正常进行。

五、校园网络管理人员应随时查看网络日志，屏蔽含有有害数据的网页。

六、全校师生不得在网络上发布不真实的信息、散布有害信息（包括计算机病毒、反动信息等）、进入未经授权使用的计算机和不以真实身份使用网络资源，禁止访问不明网站。

七、学校师生不得在网络上发布不真实的信息、散布计算机病毒、进入未经授权使用的计算机和不以真实身份使用网络资源。

八、学校师生在发现有害信息或数据时，应及时向校园网络管理人员报告，并保护现场及相关资料。

九、全校教职工应对所使用的数据做好定期备份，在紧急时刻应立即备份。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇十二**

学校校园网是为教育教学及学校管理而建立的计算机信息网络，目的在于利用先进实用的计算机技术和网络通信技术，实现校园内计算机互联、资源共享，并为师生提供丰富的网上资源。为了促进我校信息化建设和应用，提高我校现代化水平，保护校园网络系统的安全，保证校园网络的正常运行和网络用户的使用权益，更好的为教育教学服务，特制定如下管理制度。

本管理制度所称的校园网络系统，是指由校园网络设备、配套的网络线缆设施、网络服务器、工作站所构成的，为校园网络应用而服务的硬件、软件的集成系统。

1、校园网络的安全管理，应当保障计算机网络设备和配套设施的安全，保障信息的安全和运行环境的安全，保障网络系统的正常运行，保障信息系统的安全运行。

2、学校装备中心及其所辖的网络管理中心(以下简称网络中心)负责相应的网络安全和信息安全工作，定期对相应的网络用户进行有关信息安全和网络安全教育并对上网信息进行审查和监控。

3、任何单位和个人，未经网络中心同意，不得擅自安装、拆卸或改变网络设备。

4、所有上网用户必须遵守国家有关法律、法规，严格执行安全保密制度，并对所提供的信息负责。任何单位和个人不得利用联网计算机从事危害校园网及本地局域网服务器、工作站的活动。

5、进入校园网的全体学生、教职员工必须接受并配合国家有关部门及学校依法进行的监督检查，必须接受学校网络中心进行的网络系统及信息系统的安全检查。

6、使用校园网的全体师生有义务向网络中心和有关部门报告违法行为和有害信息。

1、校园网由学校装备中心统一管理及维护。连入校园网的各部门、教室和个人使用者必须严格使用由网络中心分配的ip地址。网络管理员对入网计算机和使用者进行登记，由网络中心负责对其进行监督和检查。任何人不得更改ip及网络设置，不得盗用ip地址及用户帐号。

2、与校园网相连的计算机用户建设应当符合国家的有关标准和规定，校园内从事施工、建设，不得危害计算机网络系统的安全。

3、网络管理员负责全校网络及信息的安全工作，建立网络事故报告并定期汇报，及时解决突发事件和问题。校园网各服务器发生案件、以及遭到黑客攻击后，网络中心必须及时备案并向公安机关报告。

4、对所有联网计算机要及时、准确登记备案。网络教室不准对社会开放。

5、校园网中对外发布信息的web服务器中的内容必须经领导审核，由负责人签署意见后再由信息员发布。新闻公布、公文发布权限要经过校领导的批准。

6、校园网各类服务器中开设的帐户和口令为个人用户所拥有，网络中心对用户口令保密，不得向任何单位和个人提供这些信息。校园网及子网的系统软件、应用软件及信息数据要实施保密措施。

7、加强对师生用户上网安全教育指导和监控：

(1)校园网内必须安装网络版监控和防范不良信息的过滤软件系统，监控日志至少保存半年。

(2)加强对学生开放互联网以及全校教职工上网的监管。

(3)专用的财务工作电脑和重要管理数据的电脑原则上不要接入网络工作。

8、网络中心统一在每台计算机上安装防病毒软件，各部门要切实做好防病毒措施，随时注意杀毒软件是否开启，及时在线升级杀毒软件，及时向网络中心报告陌生、可疑邮件和计算机非正常运行等情况。

9、禁止私自安装、卸载程序，在校园网上，禁止使用盗版软件，不允许玩电子游戏，不允许无关人员使用，也不允许进行与工作无关的操作，禁止任意修改和删除计算机的系统文件和系统设置。

10、严禁在校园网内使用来历不明、引发病毒传染的软件或文件;对于外来光盘、优盘、软盘上的文件应使用合格的杀毒软件进行检查、杀毒。

11、任何部门和个人不得在校园网及其连网计算机上录阅传送有政治问题和淫秽色情内容的信息。

12、未经网络中心及各子网网管的同意，不得将有关服务器、工作站上的系统软件、应用软件转录、传递到校外。

13、需在校内交流和存档的数据，按规定地址存放，不得存放在硬盘的c盘区，私人文件不得保存在工作电脑中，由此造成的文件丢失损坏等后果自负。

14、保护校园网的设备和线路，不准擅自改动计算机的连接线，不准打开计算机主机的机箱，不准擅自移动计算机、线路设备及附属设备，不准擅自把计算机设备外借。

15、各部门必须加强对计算机的管理，指定专人负责管理。管理员应经常测试计算机设备的性能，发现故障及时通知网络中心处理。

16、各部门应认真做好本部门计算机的养护和清洁卫生工作。

1、使用校园网的全体师生必须对所提供的信息负责。严禁制造和输入计算机病毒，以及其他有害数据，危害计算机信息系统的安全，不得利用计算机联网从事危害国家安全、泄露秘密等犯罪活动，不得制作、查阅、复制和传播有碍社会治安和有伤风化的信息。

2、除校园网负责人员外，其他单位或个人不得以任何方式试图登陆进入校园网服务器或计算机等设备进行修改、设置、删除等操作;任何部门和个人不得以任何借口盗窃、破坏网络设施，这些行为被视为对校园网安全运行的破坏行为。

3、用户要严格遵守校园网络管理规定和网络用户行为规范，不随意把账户借给他人使用，增强自我保护意识，经常更换口令，保护好账户和ip地址。严禁用各种手段破解他人口令、盗用账户和ip地址。

4、网络用户不得利用各种网络设备或软件技术从事用户帐户及口令的侦听、盗用活动，该活动被认为是对网络用户权益的侵犯。

违反本制度规定，有下列行为之一者，学校可提出警告、停止其上网，情节严重者给予行政处分，直至提交纪检司法部门处理，损坏的照价赔偿。

1、查阅、复制或传播下列信息者：

(1)煽动分裂国家、破坏国家统一和民族团结、违反四项基本原则的;

(2)煽动抗拒、破坏宪法和国家法律、行政法规的实施;

(3)捏造或者歪曲事实，故意散布谣言或传谣，扰乱社会秩序;

(4)公然侮辱他人或者捏造事实诽谤他人;

(5)宣扬封建迷信、淫秽、色情、暴力、凶杀、恐怖等。

2、破坏、盗用计算机网络中的信息资源和进行危害计算机网络安全的活动。

3、盗用他人帐号或私自转借、转让用户帐号造成危害者;

4、故意制作、传播计算机病毒等破坏性程序者;

5、上网信息审查不严，造成严重后果者;

6、使用任何工具破坏网络正常运行或窃取他人信息者;

7、有盗用ip地址、盗用帐号和口令、破解用户口令等危及网络安全运行与管理的恶劣行径者。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇十三**

校园网主要为我校师生员工教学、科研、管理等信息交流服务。我校校园网的管理及使用必须遵守国家的有关法律法规，达到安全、稳定、高效的目的。为了保证校园网的正常使用，特制定本管理办法。

一、校园网中的计算机设备使用对象为教职员工和全体学生。

二、校园网的使用及管理必须遵守国家的有关法律法规和行政规章制度，不得利用网络从事危害国家安全、泄露规矩秘密等犯罪活动，不得利用网络查阅、复制和传播危害国家安全、妨碍社会治安和淫秽黄色的信息。不得向学校、单位或他人发送恶意的、挑衅性的文件和商业广告。在使用因特网接入时，应遵守internet的.国际惯例和我国的有关政策，自觉不看、不传、不信各种“黄、毒、赌”及其他不良信息。

三、任何人不得在网上散布、下载、传播任何计算机病毒，一经发现将移交法律部门处理。

四、任何人不得盗用他人网址非法上网；不得盗用他人e-mail地址；不得盗用学校名义进行任何网上的非法操作。

五、任何人不准以任何理由，借助任何工具、采用任何手段擅自修改校园网中计算机终端的系统参数。安装、删除软件须经网络管理员允许。

六、对违反本管理条例的人员，学校视情节轻重给予记过以上处分，造成重大损失的将根据有关法律条文移送公安机关处理。如发现计算机硬件人为损坏，按《学校公物损坏赔偿办法》处理。

七、任何人发现网上任何异常现象（包括故障现象）都应及时与值班教师或网络中心管理人员取得联系，以便及时处理。

八、有义务和责任举报任何人的非法行为。

九、任何违规操作者一律由个人承担经济处罚和法律责任。

**校园网络安全管理制度汇编 校园网络安全管理制度 微博篇十四**

一、必须遵守《计算机信息网络国际联网安全保护管理办法》和《中华人民共和国计算机信息网络国际联网管理暂行规定》以及其它相关法律、法规的规定。

二、学校网络中心必须采取各种技术及行政手段保证网络安全和信息安全。

三、网络中心的工作人员和用户必须对所提供的信息负责。不得利用计算机联网从事危害国家安全，泄露国家秘密等违法活动，不得制作、查阅、复制和传播有碍社会治安和有伤风俗文化的信息。

四、不允许进行任何干扰网络用户、破坏网络服务和破坏网络设备的活动。包括不许在网络上发布不真实的信息，不许散布计算机病毒，不许使用网络进入未经授权使用的计算机等。

五、学校应设立网络安全员，负责网络安全和信息安全工作。

六、网络中心应按照《计算机信息网络国际联网安全保护管理办法》定期对相应的网络用户进行有关的网络安全和信息安全教育。

七、网络中心应根据国家有关规定对上网用户进行审查。凡违反国家有关规定的信息严禁上网。

八、所有用户有义务向网络安全员和有关部门报告违法犯罪行为和有害信息。

九、网络中心和用户必须接受上级有关部门依法进行的监督检查。对违反本管理办法的个人，将对其进行警告，停止网络连接、上报学校等处理。

十、安装正版杀毒软件、防火墙，按时更新杀毒软件、防火墙，定期杀毒，防范非法用户入侵，防止计算机病毒入侵。

本文档由站牛网zhann.net收集整理，更多优质范文文档请移步zhann.net站内查找