# 揭阳职业技术学院校园网管理暂行规定

（揭职院〔2006〕94号）

## 第一章　总　则

**第一条**　为加强我院校园计算机网络（以下简称校园网）的管理，规范校园网使用行为，保证校园网的正常运行与计算机信息交流的健康发展，根据《中华人民共和国计算机信息网络国际联网管理暂行规定》（中华人民共和国国务院令（第195号））、《中国教育和科研计算机网管理办法》（教技〔1996〕55号）以及其他有关管理规定，结合我院的具体情况，制定本管理规定。

**第二条**　校园网是为全校教学、科研和行政管理建立的计算机信息网络，其目的是利用先进实用的计算机技术和网络通信技术，实现校内计算机互连、计算机局域网互连，并通过中国教育和科研计算机网(CERNET)与国际互联网络(Internet)互连，实现信息的快捷沟通和资源共享。其服务对象是校属各单位和全校师生员工。

**第三条**　使用校园网的所有用户必须遵守国家和地方的有关法规以及CERNET和揭阳职业技术学院颁布的有关校园网使用管理规定。

## 第二章　组织与管理机构

**第四条**　网络中心是校园网建设与管理的组织机构，在学院的领导下，行使校园网的规划、建设、运行维护、管理与学院信息化建设的整体规划的职能。

**第五条**　各单位应有一名领导分管网络工作，对本单位网络进行监督管理，各单位的网络运行维护在网络中心的指导下，由本单位的网络管理员负责管理。

## 第三章　网络设施管理

**第六条**　校园网主干网的所有设备，包括光缆及其附属配件、路由器和交换机等属于固定资产，各入网单位和个人都应加以爱护，任何单位或个人都不能非法占用网络设备，更不能擅自拆移、盗用和破坏网络设施，发现问题应及时报告网络中心。

**第七条**　网络中心负责主干网网络设施的运行、管理和维护工作，负责对损、旧设备的拆换、变更

和其他调整工作。

**第八条** 任何单位或个人未经网络中心许可不得在主干网上私自接入新设备和变更已有入网设备，否则将追究有关单位或个人的责任。

**第九条** 网络中心负责系统机房设施的日常管理和安全管理。路由线缆、分层交换设备和接入交换设备的日常管理和安全管理由网络中心、设备所在单位共同负责管理。遇有技术故障或重要险情应立即报告网络中心。

**第十条** 需要扩充子网的单位应向网络中心提交申请和规划。未经批准，入网单位和个人不得私自扩充下级子网。各子网单位不得擅自与校外单位连网，不得擅自发展校外用户。

## 第四章 IP 地址与用户

**第十一条** 校园网的 IP 地址由网络中心负责统一管理和分配。

**第十二条** 网络中心负责办理入网用户的申请和审批手续。

**第十三条** 入网单位应统一向网络中心申请分配或增加 IP 地址。入网单位和个人应严格使用由网络中心及本单位网络管理员分配的 IP 地址，不得盗用他人 IP 地址或私自乱设 IP 地址。网络中心有权切断乱设的 IP 地址入网，以保证校园网的正常运行。

## 第五章 网络的安全管理

**第十四条** 用户在使用校园网时，必须遵守国家的有关法律、行政法规，严格执行安全保密制度。不得利用校园网和国际互联网从事危害国家安全、泄露国家秘密等违法犯罪活动，不得从事危害国家利益、集体利益和公民合法权益的活动，不得危害计算机网络和信息系统的安全。

**第十五条** 用户应严格遵守校园网管理规定和网络用户行为规范，不得在网上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，这些活动包括（但并不局限于）在网络上发布不真实的信息、散布计算机病毒、使用网络进入未经授权使用的网络资源等。

**第十六条** 各单位分管领导应做好本单位网络安全与信息安全的监督与管理工作，各单位的网络管理员应具体负责网络的安全管理。

**第十七条** 单位网络管理员须接受网络中心的业务指导，负责保存网络运行的有关记录，协助做好校园网的安全运行、管理和维护工作。

**第十八条** 校园网的工作人员和校园网的用户须接受并配合国家有关部门及学校的监督检查，须接

受并配合网络中心进行的网络系统及信息系统的安全检查。

## 第六章　网络建设与运行维护经费

**第十九条**　校园网的运行和管理收取一定的费用，以补贴校园网的正常运转费用。网络的维护、扩充、更新、改造等所需经费，由学院和所有用户按照“鼓励使用、合理分担、促进发展”的原则，采用多种方式和渠道协同解决。

**第二十条**　使用校园网的所有用户都应该根据学院相关规定按时交纳网络运行管理、通信等有关费用。

**第二十一条**　校园网运行收费办法由网络中心拟订，经学院批准后颁布执行。

## 第七章　网络信息建设

**第二十二条**　学院主页的建设由网络中心负责。

**第二十三条**　各单位可在网络中心的指导下建立自己的主页和其他专题网页，建立的网页及发布的信息必须经本单位负责人审核，网页应及时更新。

**第二十四条**　任何单位和个人未经网络中心审批，不得擅自建立网页、留言版和各种网络论坛。

**第二十五条**　用户需在校园网上公布的信息，属于学院的信息由党政办审批，属于各部门的信息由各部门审批，重要信息应该报学院领导审批，网络中心负责提供技术支持。

**第二十六条**　校园网上发布的网页由网络中心负责监督管理。

## 第八章　教育与惩戒

**第二十七条**　学院各有关部门应重视利用网络阵地，加强和改进学生的思想政治教育工作。各单位分管领导、网络管理员和各系（部）辅导员、班主任应加强对上网人员的网络道德教育，发现问题要加以引导，及时处理解决。

**第二十八条**　对于违反本规定的入网单位和个人用户，网络中心可依照情节轻重对其采取如下惩罚措施：警告，停止个人帐号，停止单机入网，停止子网入网，校纪处分，情节严重的，提交有关司法部门处理。

**第二十九条**　对违反本规定，给国家、集体或者他人财产造成损失的，应依法承担民事责任。

## 第九章　附　则

**第三十条**　本暂行规定中如有条款与国家相关法律相抵触，以国家法律为准。

**第三十一条**　本暂行规定由网络中心负责解释。

**第三十二条**　本暂行规定自发布之日起执行。

# 揭阳职业技术学院校园网安全管理办法

（揭职院〔2006〕95号）

为加强对我院网络信息安全保护，给师生员工提供一个良好的校园网络环境，杜绝网络信息安全事故的发生，确保校园网正常运行和健康发展，根据《广东省计算机信息系统安全保护管理规定》（广东省人民政府令〔2003〕81号）、《揭阳职业技术学院校园网管理暂行规定》（揭职院〔2006〕94号）和有关管理规定，结合我院实际情况，特制定本办法。

**第一条** 校园网的所有用户必须遵守《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》和国家有关法律、法规，严格执行本办法。

**第二条** 故意传播和制造计算机病毒、造成危害校园网安全的按《中华人民共和国计算机信息系统安全保护条例》的规定予以处罚。

**第三条** 任何单位和个人不得利用校园网制作、复制、查阅和传播下列信息：

（一）煽动抗拒、破坏宪法和法律、行政法规实施的；

（二）煽动颠覆国家政权，推翻社会主义制度的；

（三）煽动分裂国家、破坏国家统一的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）捏造或者歪曲事实，散布谣言，扰乱社会秩序的；

（六）宣扬封建迷信、淫秽、色情、赌博、暴力、凶杀、恐怖，教唆犯罪的；

（七）公然侮辱他人或者捏造事实诽谤他人的；

（八）损害学院形象和学院利益的；

（九）其他违反宪法和法律，行政法规的。

**第四条** 凡属国家秘密文件、资料一律不得输入计算机互联网络；本单位、本部门科学研究方面的文件、资料、成果必须依据国家《科学技术保密规定》和《科技成果密级评定方法》进行确定，如属国家秘密范围，不得进入互联网。各单位、各部门涉密人员必须做好资料及涉密科研项目、成果的保管工作，把好保密源头。各单位、各部门要加强对信息存储介质（软盘、磁带及光盘）的管理，对存储有秘密文件、资料的计算机及外围要有专人或兼职人员操作，采取必要的防范措施，建立规范的管理制度。

**第五条** 机要部门及重要部门的要害信息系统的联网，应重点加强信息网络安全管理和保卫工作。

**第六条** 校园网所有工作人员和用户发现违法案件、有害信息、病毒引起的计算机信息系统瘫痪，程序、数据严重破坏等事故的，必须立即向网络中心和保卫科报告并由保卫科向公安局备案。网络中心

须积极做好协助查处工作，及时做好有关信息的保存、清除与备份工作。

**第七条** 在校园网上不允许进行任何干扰网络用户、破坏网络服务和网络设备的活动。

**第八条** 各单位用户应定期对其服务器、网站备份（1 个星期 1 次），特殊单位按照各自情况安排备份工作。

**第九条** 各单位用户应建立以下安全管理制度：

（一）安全管理责任制度。指定信息安全责任人，明确本单位工作人员的安全管理职责。

（二）安全保护制度。保障信息安全，保障计算机网络设施、信息系统、设施和运行环境安全，保障计算机功能正常发挥。

（三）安全操作制度。规定信息网络系统的操作权限和程序。

（四）安全检查制度。应定期对其服务器、上网计算机进行信息安全检查。对系统的安全漏洞，必须及时采取措施加以解决。

（五）安全审核制度。开设电子公告版及公共留言版等公共网络交流平台的单位，要完善登记备案及信息审核制度。

**第十条** 任何单位或个人不得在网上发送邮件炸弹和扫描网络端口，不得盗用他人帐号和通过网络窃取他人信息，不得利用黑客技术非法进入任何未经授权的网络系统和信息系统；任何单位或个人不得私自提供 WWW、FTP、DHCP、DNS、BBS 和网络代理等服务，不得利用或变相利用校园网资源从事商业活动。

**第十一条** 用户入网，必须办理入网申请手续，按规定认真填写用户入网申请表，并与网络中心签订入网安全协议。校园网用户一律采用实名注册上网。注册用户应妥善保管自己的账户，不得以任何形式转借他人。因转借账号、账号丢失或被盗用而未及时到网络中心备案，给校园网络及网络信息安全造成损失的，将视情节轻重追究账号注册者及其相关人员的责任。

**第十二条** 各单位与个人的合法权益受保护，校园网不允许任何侵权行为。

**第十三条** 校园内从事的施工、建设等工程不得危害校园网系统的安全运行，如发生问题应及时报告网络中心。

**第十四条** 学生寝室之间、教学实验室之间不得私拉乱接网络线，不得私自架设有路由功能设备，不得在校园私自使用 ADSL 等非校园网线路访问网络。

**第十五条** 提供上网的公共机房要严加管理，机房负责人为网络安全负责人，上网人员必须出示合法证件，机房工作人员严格记录上网人员的身份和上网时间、机号、IP 地址，公共机房网络使用记录至少保留一年。

**第十六条** 已经审核批准提供服务的网站、服务器须具有日志记录功能，保存用户访问记录至少 3

个月。

**第十七条** 校园网的所有管理人员和用户有义务配合网络中心及相关职能部门依法对校园网进行监督检查。

**第十八条** 每个上网用户应自觉遵守本办法。一经发现有违反本办法，网络中心将视其情节轻重，给予有关责任人以下处分：

（一）警告并勒令改正；

（二）网上通报批评；

（三）中止其网络服务 3 至 90 天（不予退款）；

（四）取消账户，并记入重点监控黑名单（不予退款）；

（五）由有关部门给予相应处分；

（六）移交公安机关处理。

**第十九条** 本办法包括但不局限于本办法的所有内容，未尽事宜将按国家、省、市和学院有关规定执行。

**第二十条** 本办法由网络中心负责解释。

**第二十一条** 本办法自发布之日起执行。

# 揭阳职业技术学院校园网使用收费管理办法

（揭职院〔2007〕18号）

**第一条** 为加强我院校园网的统一管理，保证校园网的良性运行和健康发展，更好的促进校园信息化建设，根据中国教育和科研计算机网(CERNET)的有关规定，结合我院实际情况，本着“鼓励使用、合理分担、促进发展”的原则，制定本管理办法。

**第二条** 我院校园网由学院投资建设，面向全院的教学、科研、管理和广大教职员工、学生服务，实行有偿使用。使用校园网的所有用户，应遵循本管理办法，并及时缴交有关费用。

**第三条** 凡办理入网的新用户，须携带本人身份证或工作证或学生证等有效证件到学院网络中心领取并填写开户申请表。

**第四条** 用户自愿入网，入网方式为先交费后使用，每学期交费一次，中途退网不予退款。新用户持开户申请表、老用户直接到财务处缴交所需费用，凭缴费收据再到网络中心办理上网充值。

**第五条** 收费标准：

| 收费项目 | 收费标准 | 收费范围及对象 | 说明 |
| --- | --- | --- | --- |
| 校园网使用费 | 40元/帐号/每学期 | 所有校园网用户 | 免费开户 |

**第六条** 学期中途退网不予退回所交费用，中途入网，仍按一个学期的标准交费。

**第七条** 用户需要临时停用帐号时，须携带有效证件到网络中心办理手续,所交费用不予退回。

**第八条** 学生用户毕业离校前须以班为单位到网络中心办理帐号注销手续。教工用户调离学校时，须按照教工用户注销帐号办法办理相应手续。

**第九条** 个人申请的帐号不得转借或与他人共用，帐号密码必须经常修改并注意保密，如被他人使用而产生的一切经济和法律责任，由帐号持有人承担责任。

**第十条** 用户如发生上网故障请及时通知网络中心，经调查，如属校园内部网络线路、服务器及交换机出现故障，网络中心原则上在三天内给予解决；如属用户个人原因，则自行解决。

**第十一条** 校园网所有的收费原则上用于支付CERNET和CHINANET的网络分担费（月租及国际流入费用）和校园网资源（各种网络设备、IP地址及各种软件）的购买、管理、维护和开发等的费用。

**第十二条** 本管理办法由网络中心负责解释。

**第十三条** 本管理办法自2007年2月1日起执行。

# 揭阳职业技术学院短信服务平台管理办法

（揭职院〔2007〕35号）

为加强对我院短信平台的管理，杜绝用户利用短信平台传播违法违规信息的事故发生，充分发挥短信平台的效益，更好的促进校园信息化建设，特制定本管理办法。

一、本管理办法中的短信服务平台是指由网络中心建设、管理并提供校内服务的短信发送平台。

二、各使用部门要严格遵守《互联网信息服务管理办法》，建立健全内部保障制度、信息安全管理制度。

三、各使用部门要建立健全信息安全责任制度和信息发布的审批制度，严格审查通过本平台所发布的短信内容，保证信息内容的健康、合法。

四、任何人不得利用短信平台制作、复制、发布、传播含有下列内容的信息：

（一）反对宪法所确定的基本原则的；

（二）危害国家安全，泄露国家秘密，颠覆国家政权，破坏国家统一的；

（三）损坏国家荣誉和利益的；

（四）煽动民族仇恨、民族歧视，破坏民族团结的；

（五）破坏国家民族宗教政策，宣扬邪教和封建迷信的；

（六）散布谣言，扰乱社会秩序，破坏社会稳定的；

（七）散布淫秽、色情、赌博、暴力、凶杀、恐怖或者教唆犯罪的；

（八）侮辱或者诽谤他人，侵害他人合法权益的；

（九）含有法律、行政法规禁止的其他内容的；

五、针对部门内部应用的相关业务，明确用户群和用户范围，手机用户必须是自愿接受服务，不得向陌生用户随意发送任何无关信息。

六、发送短信的内容必须真实、准确，不许有任何玩笑以及其他与工作无关信息，发送的短信必须署上发送该短信的部门名称。

七、部门帐号要由专人管理、专人使用，并不得借给其它人员使用，严格保护好帐号与密码的安全。

八、部门帐号管理人员调离岗位时，本部门应该重新指定一个帐号管理员，并到网络中心进行部门帐号管理人员更改备案、重新设置用户名和密码。

九、短信平台管理员有权对用户传输的短信内容进行监控，如发现有违反以上规定的情况，学院将取消其继续使用服务平台的资格，并追究其部门负责人的相关责任。

十、部门用户开户（预充短信）申请流程为：单位用户提出申请→网络中心审批→网络中心主管领导审批→网络中心开通（预充）。

十一、本办法由网络中心负责解释。

十二、本办法自发布之日起执行。

# 揭阳职业技术学院校园网运营管理暂行办法

（揭职院〔2010〕101 号）

**第一条** 根据中国教育和科研计算机网的费用分摊政策，按照《揭阳职业技术学院与中国电信股份有限公司揭阳分公司（下称揭阳电信），广州泰昌科技有限公司关于校园网三方合作协议》中的有关条款，结合学院实际情况制定本暂行办法。

**第二条** 本暂行办法适用于校园内网络用户。

**第三条** 校园网的运营方式

（一）与揭阳电信合作后校园网由学院与揭阳电信共同出资建设。

（二）校园网面向全院师生，服务于教学、科研和管理，实行有偿使用。

（三）校园网由学院、揭阳电信及第三方代理公司共同运营，所收取费用按比例分成。

**第四条** 收费管理办法

（一）收费原则

1.按照先交费后使用，实行合理收费、维持运行、控制浪费、优化服务，达到发挥效益、服务于教学科研的目的。

2.用户自愿入网，每学期缴费一次，中途退网不予退费。新用户持开户申请表、老用户直接到指定地点缴费，凭缴费收据到网络中心办理入网、充值等手续。

3.中途入网按照剩余月份比例缴费。

4.学生毕业及教职工调离后账户自动注销，费用不予退还。

（二）用户分类

根据学院的实际情况，将用户分为以下几类：

1.个人用户。是指需要办理信息点开通手续并申请用户账号的学生宿舍和教职工住宅内的用户。

2.单位用户。是指通过学院办公区内接入的用户，办公区包含学院行政综合楼、图书馆非机房部分、教学楼内部分办公室、实训大楼及实训大楼扩建一期以及以后新增建筑内的办公区。

3.开放式机房。是指从院内计算机机房、网络机房非办公部分、电子阅览室、多媒体教室等接入的用户。

（三）收费方式：由代理公司进入学院定点、定时进行收费，每半年收取一次并进行三方结算。

（四）收费标准

1.个人用户

（1）个人用户采用账号管理方式，每用户一个账号，根据用户选择的带宽差别收费；

（2）每账号独享 2M 带宽，收取每学期 70 元、每学年 140 元；

（3）每账号独享 4M 带宽，收取每学期 100 元、每学年 200 元；

2.单位用户及开放式机房

（1）单位用户及开放式机房采用网络直连方式，用户可以直接接入。

（2）每账户独享 2M 带宽（网络中心机房内用户不限带宽，机房内用户包含机房内所有需要提供对外服务的服务器）。

（3）单位用户及开放式机房用户根据合作协议每年定额收取，于每年第一次结算费用时进行结算。

**第五条** 学院按照比例分成所得费用原则上专款专用，即用于日常网络维护、网络设备更新以及各种网络软硬件资源的购置、开发等。

**第六条** 本管理办法由网络中心负责解释。

**第七条** 本暂行办法自发文之日起执行。揭职院〔2007〕17 号文不再执行。

# 揭阳职业技术学院网络信息管理暂行办法

（揭职院〔2014〕146号）

## 第一章　总　则

**第一条** 为切实加强学院网络信息管理，确保网上信息规范、有序,引导正确的宣传与舆论导向，进一步促进学院网站的正常运行和健康发展，特制定本暂行办法。

**第二条** 学院宣传统战部为学院网络信息的主管部门，学院网站为学院网络信息的主要载体。

**第三条** 学院网站由学院主网站、二级网站（包含各职能部门、各系部网站、其他机构独立网站及教师和学生个人网站）。

**第四条** 本办法适用于学院网站含二级网站内的所有信息。

## 第二章　网络信息的内容

**第五条** 学院主网站上的内容要突出重点，反映全学院重要的、综合的、宏观的信息。学院主网站信息主要包括以下内容：

(一)政务工作、信息及动态；

(二)职能部门、系部经常性业务工作信息；

(三)招生就业、科学研究等业务工作信息；

(四)其他教师、学生类信息。

**第六条** 学院二级网站栏目设置可包括以下内容：

(一)反映本部门工作职能、职责的信息，包括部门职责、业务简介、人员构成、部门荣誉以及各类规章制度、管理办法、文件等；

(二)反映本部门工作的动态信息，包括工作计划、总结、工作动态等；

(三)其它有关本部门的专业知识和高职教育信息等。

**第七条** 学院主网站信息内容与各院属职能部门、系（部）网站信息内容是相互依存、相互补充的。院属职能部门、系（部）网站建设，要服从学院主网站建设的统一要求，要互相支持、积极配合，共同搞好全院网站的建设。

## 第三章　信息的管理与维护

**第八条** 宣传统战部负责主网站内容建设、网上舆论引导、网络文化建设等全面管理工作；各职能部门、系（部）网站信息由各部门、系（部）负责管理其相应工作范围内的板块内容；团委负责管理学生类板块信息。

**第九条** 网络中心负责信息系统技术维护和技术培训等方面的工作。主要职责为：

（一） 负责学院主网站及相应校级网络应用系统的开发和建设；设计、制作和维护学院主页，协助设定网上栏目并对有关栏目进行维护；

（二）提供技术支持，负责校级公共数据库等基础系统运行、维护和管理工作；

（三）协助制定学院网络信息工作计划和具体规章制度；

（四）协助宣传统战部审定各职能部门、系（部）单位网络建设和管理信息系统开发、建设方案及上网主页内容，协助指导、协调、监督和考核各部门网络信息工作；

（五）负责为校园网用户、学院各部门信息工作人员提供技术咨询、技术服务和有关培训。

**第十条** 二级网站网络信息实行部门负责制。各职能部门、系（部）网络信息工作的主要职责为：

（一）根据学院网络信息工作计划，制定本部门网络信息工作计划，并组织实施；

（二）贯彻落实学院网络信息工作有关规定，制定本部门网络信息工作管理办法，并组织落实；

（三）按照学院统一规划的要求，负责本部门信息网站及管理信息系统的建设；

（四）设计、制作和维护本部门上网主页，设定网上栏目，按规定程序报审本单位上网内容，按照学院要求进行维护，搞好本部门上网信息的管理；

（五）完整、准确地建立本部门基础信息集，及时向学院主网站提供本部门上网信息，为更新学院网上公共信息和对外发布信息服务，并做好有关宣传工作；

（六） 切实按照学院有关规定和要求，选派好本部门网络信息工作负责人和网络信息员，为网络信息工作创造必要的条件，检查、督促网络信息工作人员认真履行规定的职责，并加强对网络信息工作的指导；

（七）认真组织好本部门上网用户的培训工作。

## 第四章　信息的审核与监控

**第十一条** 学院网络信息的审核实行分级负责制。

一、宣传统战部：

（一）负责学院网站上的各类信息的全面把关审核。对各职能部门、系（部）已上网发布的信息进行巡查和监督，切实做好学院对外宣传工作和网上舆论引导；

（二）负责学院网站上的各类信息的全面监控。发现有害、不良信息应及时联合学院网络中心的技术人员进行原始信息记录的制止、删除，查处对管辖区域内违反有关规定的人或事；

二、各职能部门、系（部）负责对各自发布在学院网站及本部门网页上的各类信息进行把关,责任到人。发布在网上的信息，除按正常工作程序在上网前进行审核把关外，在加载完后要将网上信息进行对照检查，加载过程中发现的错误要及时更正。要保证网上资料与同类有关资料、文件准确一致，没有错误、遗漏、重复、数据丢失等现象。

三、学院教师、学生等其他个人对各自发布的信息文责自负。

**第十二条** 网络信息管理人员及用户在所有与校园网相关的活动中按规定必须接受国家安全机关、公安机关、保密机关、学院保卫部门、上级网络信息管理单位的管理和监督。

**第十三条** 加强校园网络突发事件应急预案建设，一旦发生网络突发事件，要做到快速反应、有效处置。

## 第五章 信息的考核

**第十四条** 学院网站的各种信息资料要根据实际工作情况进行定期维护，对各种数据及不定期文字资料，各部门要根据工作完成情况随时进行更新、加载，保证其准确性和及时性。

**第十五条** 宣传统战部定期对各部门网上提供的各种动态资料、信息等加载情况进行检查，年终对各种相对固定栏目资料加载情况进行汇总。

**第十六条** 宣传统战部每年组织一次各部门上网信息评比，第十五条的统计结果作为评比的主要依据之一,表彰优秀网络信息工作部门、优秀网络信息工作负责人、优秀网络信息员。对考核不合格部门进行公布并要求限时整改。

## 第六章 附 则

**第十七条** 本办法由宣传统战部、网络中心负责解释，并对本办法的执行情况进行监督检查。

**第十八条** 本办法自公布之日起执行，与本办法相抵触的，以本办法为准。

# 揭阳职业技术学院数据共享与安全管理办法

（揭职院〔2021〕121 号）

## 第一章 总则

**第一条** 为加强揭阳职业技术学院信息化数据的统一规划管理，推动数据共享，确保数据安全，根据《中华人民共和国网络安全法》及《中华人民共和国数据安全法》等法律法规，制定本管理办法。

**第二条** 揭阳职业技术学院信息化数据作为学校的无形资产和资源（以下简称数据），应纳入学校统一管理范畴，实现数据的统一管控，提高数据质量和数据的利用效率，提供安全、完整、统一的数据服务，为学校教学、科研、管理提供信息服务和技术保障。

**第三条** 本管理办法所涵盖的数据范畴，主要是指揭阳职业技术学院内部有关教学、科研、管理方面的各信息化数据。管理的对象主要是由信息系统运行过程中产生的数据、使用计算机编制的数据、专业系统采集的原始数据等，包括各类文本数据、数据库数据、WEB 页面信息、图形图像数据(包含人脸识别图像数据)、多媒体数据等结构化数据、半结构化数据和非结构化数据。

## 第二章 数据的管理和使用

**第四条** 学校各部门本着“谁产生数据，谁负责管理”的原则，信息化数据产生部门负责本部门数据的采集、使用、维护、归档和备份的全周期管理。各部门主要负责人为信息化数据管理第一责任人。

**第五条** 学校信息化数据管理职能部门（下称职能部门）为实训与信息中心，负责统筹规划全校信息化数据管理工作。包括学校信息化数据资源的总体规划，数据标准、编码标准、技术规范、管理规范的制定；负责各类异构数据源的整合，对外提供统一的访问接口和数据服务；学校数据中心公共数据的使用、维护、存储、备份和恢复等。

**第六条** 各业务系统产生的基础数据均归揭阳职业技术学院所有，任何部门无权独占，各业务系统数据应遵从学校统一数据标准规范设计，数据生产部门有义务确保各自所维护数据的及时性和准确性，按照学校数据中心的接口标准向数据中心共享数据。

**第七条** 学校为各部门提供统一的数据交换接口。数据使用部门需根据自身需求，向职能部门提出数据使用申请，职能部门审核批准后向数据使用部门提供数据交换接口。

## 第三章 数据中心建设与管理

**第八条** 建立数据中心是实施数据整合、进行有效数据管理的基本策略。数据中心是各部门发布、

访问、共享数据的工作平台。数据中心由学校统一建设，并将各部门内自管数据、部门间共享数据、外购数据全部接入数据平台，并实施数据整合。各部门有责任支持和配合数据中心的建设工作。

**第九条** 学校职能部门负责数据中心管理和服务，有义务组织各业务部门进行内部业务数据的需求分析，各业务部门依据业务职能提出各种内部数据需求，并分别按本部门内自管数据、需要其他部门提供的数据分别汇总，确定数据内容、数据同步周期和数据提供方式等。

**第十条** 学校职能部门组织汇总各业务部门需要其他部门提供的数据，建立全校数据中心，对各种数据进行归类。对各部门间共享数据，理顺数据来源和数据使用渠道，并分别反馈给各相关部门核对认可。

**第十一条** 跨业务系统的数据共享应根据需求，由学校职能部门协调共享数据资源，各业务部门有义务实时提供本部门业务系统所产生的权威数据到学校数据中心。各业务系统可以从数据中心获取到所需要的基础数据和业务变更数据。

**第十二条** 学校职能部门负责数据中心的运行和维护，及时进行数据的收集、清洗、整理、分发等处理，保证数据的畅通交流、充分共享。

## 第四章 数据维护与安全

**第十三条** 在各类信息系统中，应严格按照岗位设置数据维护权限，规范权限的分配和管理。严禁在未按规定授权的情况下委托他人以本人的账户和口令进行有关的数据录入和修改。各系统用户应当定期更改自己的口令，保证数据的安全。

**第十四条** 学校各相关部门应在职能部门的指导和协助下，结合本部门实际情况，定期做好数据维护与规范管理，明确数据维护的权限和职责，制定数据维护的规程。

**第十五条** 学校职能部门负责制定和实施数据中心数据统一存储、管理、备份和容灾方案，各业务部门负责业务系统的数据存储、管理、备份和容灾方案。

**第十六条** 各部门和系统管理人员，要对自己所管理的数据负责，保证数据安全，防止数据泄露。学校数据信息主要用于教学、科研、管理、生活服务等，申请数据获取的部门有义务保护数据的隐秘性，不得将数据信息用于申请用途外的活动。

**第十七条** 未经批准，任何单位和个人不得擅自对外提供信息系统的内部数据，应保护师生个人隐私信息，保障教育数据资源安全。未经学校审批，严禁将学校业务数据与校外系统交换，不得将获取的共享数据资源挪作他用，不得以任何方式用于社会有偿服务或其他商业活动。

**第十八条** 对于违反本管理办法有关规定，擅自泄露或篡改信息系统中的数据，将数据信息用于申请用途以外的活动，造成损失的部门或个人，按照相关规定，视情节轻重，给予相应处分。

**第十九条** 对于有危害公共安全、国家安全、泄露国家秘密以及其他违反法律、法规和规章规定行为的，由公安、国家安全、保密以及其他监督管理等国家相关部门依法处理；涉嫌犯罪的，移送司法机关，依法追究刑事责任。

## 第五章 附则

**第二十条** 本办法由实训与信息中心负责解释，自印发之日起实施。

# 揭阳职业技术学院网络与信息安全事件应急预案

一、总则

（一）编制目的

建立健全学校网络与信息安全事件应急工作机制，提高应对网络与信息安全事件能力；预防和减少网络与信息安全事件造成的损失和危害，维护学校、国家安全和社会稳定。

（二）编制依据

依据《中华人民共和国突发事件应对法》、《国家网络与信息安全事件应急预案》,《信息安全事件分类分级指南》

（GB/Z 20986—2007),《广东省突发事件应对条例》、《广东省突发事件总体应急预案》、《广东省网络与信息安全事件应急预案》等法律法规及有关规定，制定本预案。

（三）适用范围

本预案适用于全校网络与信息安全事件的预防和处置工作。

二、术语和定义

本预案所称的网络与信息系统，是指由揭阳职业技术学院校园网络、计算机及其相关的和配套的设备、设施构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

本预案所称的网络与信息安全事件是指由于自然或者人为以及软硬件本身缺陷或故障的原因，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件。

网络与信息安全事件分为网络攻击事件、设备故障事件、灾害性事件、信息内容安全事件等 4 个基本分类。

三、处置原则

网络与信息安全事件应急处置，依照“统一领导，快速反应，密切配合，科学处置”的组织原则和“谁主管谁负责、谁运行谁负责、谁使用谁负责”的协调原则，充分发挥各方面力量，共同做好网络与信息安全事件的应急处置工作。

四、工作原则、组织机构及职责

（一）预防为主、平战结合

坚持事件处置和预防工作相结合，做好事件预防、预判、预警工作，加强应急支撑保障能力和安全态势感知能力建设。提高网络安全事件快速响应和科学处置能力，抓早抓小，争取早发现、早报告、早

控制、早解决，严控网络安全事件风险和影响范围。

（二）学校网络与信息安全事件应急处置工作由学校网络安全与信息化领导小组统一指导、指挥、协调。机构组成如下：

组 长：李文升

常务副组长：龚善初

副组长：姚玉平、李桂鑫、刘瑞叶

成 员：各系（部、院）、各部门责人，各党总支部、直属支部负责人。领导小组下设信息安全办公室及技术安全办公室。信息安全办公室日常工作由宣传统战部负责；技术安全工作办公室日常工作由实训与信息中心负责。各相关单位须坚决执行领导小组的决定，密切配合，履行职责。

（三）相关部门职责

1.宣传统战部：负责学校校园网意识形态安全工作，负责与上级网信办联系。

2.财务处：按照有关规定，为网络与信息安全事件应急处置和实施重要保障任务提供必要的经费保障。

3.后勤服务处：负责协调提供相关应急物资装备。

4.实训与信息中心：负责打击学校网络攻击破坏和包括计算机病毒在内的恶意代码传播等活动的应急协调工作；负责学校网络信息系统基础设施、设备的网络与信息安全事件的预防、监测、报告、应急处置和保障工作。负责与上级教育部门、公安网警部门联系。

5.其他部门：负责本部门内部的网络与信息安全管理和突发事件应急处置；对照本预案建立单位内部应急处置机制；配合各部门落实相关应急处置措施。

五、应急响应与处置

（一）事件分级

根据可能造成的危害、可能发展蔓延的趋势，网络安全事件分为四级：特别重大网络安全事件(Ⅰ级)、重大网络安全事件(Ⅱ级)、较大网络安全事件较大(Ⅲ级)、一般网络安全事件一般Ⅳ级)。

1.符合下列情形之一的，为特别重大网络安全事件（Ⅰ级）：

(一)学校网络与信息系统发生全校性大规模瘫痪，对学校正常工作造成特别严重损害，且事态发展超出学校控制能力的安全事件；

(二)学校核心业务信息系统（网站）的重要敏感信息或关键数据丢失或被窃取、篡改，且事态发展超出学校控制能力的安全事件；

(三)其他对学校安全稳定和正常秩序构成特别严重威胁，造成特别严重影响的网络安全事件。

2.符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件（II 级）：

(一)学校网络与信息系统造成全校性瘫痪，对学校正常工作造成严重损害，事态发展超出学校信息技术部门控制能力，需学校各部门协同处置的安全事件；

(二)学校核心业务信息系统（网站）遭受严重系统损失，造成系统瘫痪，业务处理能力受到重大影响；

(三)核心业务信息系统（网站）的重要敏感信息或关键数据发生丢失或被窃取、篡改；

(四)其他对学校安全稳定和正常秩序构成严重威胁，造成严重影响的网络安全事件。

3.符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件（III 级）：

(一)学校某一区域的网络与信息系统瘫痪，对学校正常工作造成较大损害的安全事件；

(二)重要业务信息系统（网站）遭受较大系统损失，明显影响系统效率，业务处理能力受到影响；

(三)重要业务信息系统（网站）的信息或数据发生丢失或被窃取、篡改、假冒；

(四)其他对学校安全稳定和正常秩序构成较大威胁，造成较大影响的网络安全事件。

4.一般(Ⅳ级)

一般网络安全事件（IV 级）：除上述情形外，对学校安全稳定和正常秩序构成一定威胁、造成一定影响的网络安全事件，为一般网络安全事件。

（二）报告程序

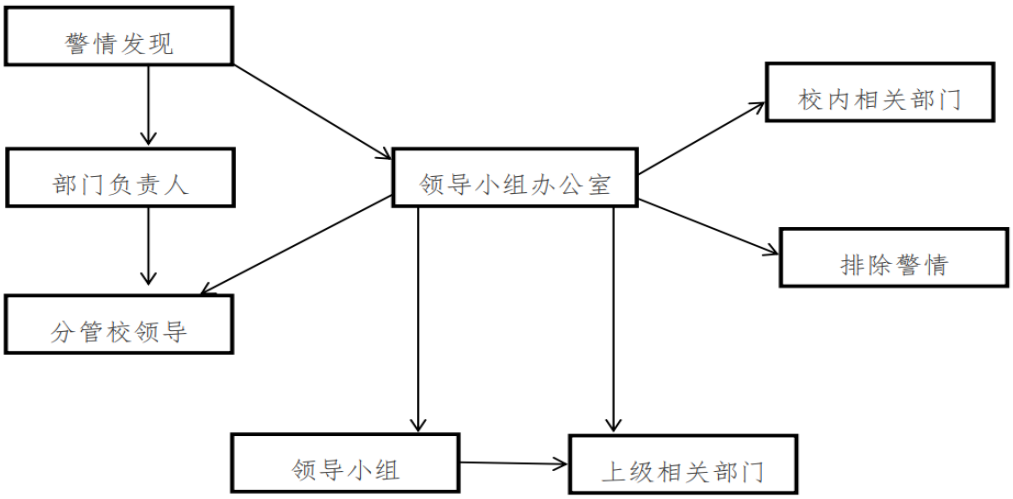
1.各单位（部门）监测人员一旦发现网络与信息安全事件，应立即采取措施控制事态影响，及时进行风险评估，并向领导小组办公室及本部门负责人报告。

2.对于发生一般(Ⅳ级)级别的网络与信息安全事件，由领导小组办公室处理，并将处理情况分别向分管校领导和领导小组报告。

3.对于发生较大(Ⅲ级)、重大(Ⅱ级)、特大(Ⅰ级)的网络与信息安全事件，由领导小组办公室第一时间向领导小组报告。领导小组接到报告后，根据上级有关规定向相关上级部门报告，并迅速召开会议，研究确定网络与信息安全突发事件的态势及研究应急处置方案。

情况报告内容包括：灾害发生的时间、地点，灾害的性质，灾害的级别及影响范围，采取应急处置方案等。

报告流程图如下：




（三）处置措施

1. 根据网络与信息安全事件分类采取不同应急处置方式。

（1）网络攻击事件：判断攻击的来源与性质，关闭影响安全与稳定的网络设备和服务器设备，断开信息系统与攻击来源的网络物理连接，跟踪并锁定攻击来源的 IP 地址或其它网络用户信息，修复被破坏的信息，恢复信息系统。按照事件发生的性质采取以下方案：

病毒传播：及时寻找并断开传播源，判断病毒的类型、性质、可能的危害范围；为避免产生更大的损失，保护健康的计算机，必要时可关闭相应的端口，甚至相应楼层的网络，及时请有关技术人员协助，寻找并公布病毒攻击信息，以及杀毒、防御方法。

外部入侵：判断入侵的来源，区分外网与内网，评价入侵可能或已经造成的危害。对入侵未遂、未造成损害的，且评价威胁很小的外网入侵，定位入侵的 IP 地址，及时关闭入侵的端口，限制入侵的 IP 地址的访问。对于已经造成危害的，应立即采用断开网络连接的方法，避免造成更大损失和影响。

内部入侵：查清入侵来源，如 IP 地址、所在办公室等信息，同时断开对应的交换机端口，针对入侵方法调整或更新入侵检测设备。对于无法制止的多点入侵和造成损害的，应及时关闭被入侵的服务器或相应设备。

（2）设备故障事件：判断故障发生点和故障原因，迅速抢修故障设备，优先保证校园网主干网络和主要应用系统的运转。

（3）灾害性事件：根据实际情况，在保障人身安全的前提下，保障数据安全和设备安全。具体方法包括：硬盘的拔出与保存，设备的断电与拆卸、搬迁等。

（4）信息内容安全事件：接到校内网站出现不良信息的报案后，应迅速屏蔽该网站的网络端口或拔掉网络连接线，阻止有害信息的传播，根据网站相关日志记录查找信息发布人并做好善后处理；对公安

机关要求我校协查的外网不良信息事件，根据校园网上网相关记录查找信息发布人。

（5）其它不确定安全事件：可根据总的安全原则，结合具体情况，做出相应处理。不能处理的及时咨询信息安全公司或顾问。

2.后续处理

（1）安全事件进行最初的应急处置后，应及时采取行动，抑制其影响进一步扩大，限制潜在的损失与破坏，同时要确保应急处置措施对涉及的相关业务影响最小。

（2）安全事件被抑制后，通过对有关事件或行为的分析结果，找出问题根源，明确相应补救措施并彻底清除。

（3）在确保安全事件解决后，要及时清理系统，恢复数据、程序、服务，恢复工作应避免出现误操作导致的数据丢失。

3.记录上报

网络与信息系统安全事件发生时，应及时向校领导和校园网络与信息安全事件应急处置领导小组汇报，并在事件处置工作中作好完整的过程记录，及时报告处置工作进展情况，保存各相关系统日志，直至处置工作结束。

4.结束响应

系统恢复运行后，要对事件造成的损失、事件处理流程和应急预案进行评估，对响应流程、预案提出修改意见，总结事件处理经验和教训，撰写事件处理报告，同时确定是否需要上报该事件及其处理过程，需要上报的应及时准备相关材料；属于重大事件或存在非法犯罪行为的，第一时间向公安机关网络监察部门报案。

六、应急处置

（一）网络安全事件发生后，事发单位应立即启动应急预案，立即组织本单位的应急队伍和工作人员根据不同的事件类型和事件原因，采取科学有效的应急处置措施，尽最大努力将影响降到最低，并注意保存网络攻击、网络入侵或网络病毒等证据。

（二）事发单位技术能力无法处置的，应及时通报领导小组办公室。由领导小组办公室研判，认定为特别重大网络安全事件的，报领导小组、教育部网络安全应急办公室、市网警。对于人为破坏活动，同时由宣传统战部报当地公安机关。

七、调查与评估

（一）特别重大网络安全事件由领导小组办公室组织有关单位开展调查处理和总结评估工作，并将调查评估结果汇总上报领导小组及市网警领导；重大网络安全事件根据事发单位属性，由领导小组办公室组织开展调查处理和总结评估工作；较大和一般网络安全事件由领导小组办公室开展调查处理和总结

评估工作。

（二）网络安全事件总结调查报告应对事件的起因、性质、影响、责任等进行分析评估，提出处理意见和改进措施。网络安全事件的调查处理和总结评估工作应在应急响应结束后 5 天内完成。

八、预防工作

（一）各单位应做好网络安全事件日常预防工作，根据本预案制定完善相关的专项应急预案和配套的管理制度，建立完善的应急管理体制。按照网络安全等级保护、关键信息基础设施防护等相关要求落实各项防护措施，做好网络安全检查、风险评估和容灾备份，加强信息系统的安全保障能力。

（二）各单位应加强网络安全监测预警和通报，及时发现并处置安全威胁。领导小组办公室应全面掌握学校信息系统（网站）情况，建立学校网络安全监测预警和通报机制，并指导、监督学校二级单位及时修复安全威胁，全面排查安全隐患，提高发现和应对网络安全事件的能力。

（三）领导小组办公室负责每年组织针对特别重大网络安全事件的跨层级的应急演练，检验和完善预案，提高实战能力。每年至少组织一次应急演练，每年年底前将本年度演练情况报市网警领导。

（四）各单位应加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传教育。同时，充分利用网络安全周等各种活动形式和传播媒介，开展网络安全基本知识和技能的宣传活动，提高本单位师生的网络安全意识。

（五）各单位应定期组织网络安全培训，将网络安全事件的应急知识列为领导干部和有关人员的培训内容，加强网络安全。特别是网络安全事件应急预案的学习，提高网络安全管理和技术人员的防范意识及安全技能。

九、保障措施

（一）队伍保障

加强队伍建设，定期对相关工作人员进行网络与信息系统安全知识培训，不断提高安全岗位工作人员的信息安全防范意识和技术水平，增强预防意识和应急处置能力，有针对性地开展应急演练，确保相关措施有效落实，确保安全事件处置得当。

（二）技术保障

不断完善网络安全整体方案，加强技术管理，确保信息系统的稳定与安全。

（三）资金保障

学校应根据校园网络与信息系统安全预防和应急处置工作的实际需要，制订年度应急处置工作相关设备和工具所需经费预算，纳入年度预算并给予资金保障。

七、预案实施

本预案自发布之日起实施。