第一章总则

第一条 为加强北京师范大学-香港浸会大学联合国际学院（以下简称：UIC）校园网络及相关基础设施的建设和管理，保障学校相关工作的有序发展，根据《中华人民共和国网络安全法》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《中华人民共和国计算机信息网络国际联网安全保护管理办法》和《中国教育和科研计算机网暂行管理办法》等有关规定，结合我校实际情况，特制定本办法。

第二条 UIC 校园网（以下简称校园网）由学校投资建设，是学校教学、科研、管理和服务的信息基础设施，是学术性、非赢利性的计算机网络。校园网覆盖范围包括教学、科研和行政管理等区域。校园网的服务对象是学校各单位、师生员工以及其他经学校许可的单位和个人。

第三条 校园网相关基础设施是指学校校园建筑范围内，由学校投资建设的管道、管线、机房、弱电间、综合布线系统和有线无线网络等设施以及由运营商投资建设的管道、管线、传输线路、通信机房和基站等通讯设施。

第四条 校园网的所有用户必须遵守国家有关法律、法规，遵守公共秩序，尊重社会公德，不得危害网络安全，严禁使用校园网从事违法违纪的网络活动，使用人需对自身提供的网络信息负责。

第五条 未经批准，任何单位和个人不得将校园网延伸至校外或将校外网络引入至校园内，不得利用校园网开展赢利性经营活动。未经批准，任何数据业务运营商或代理商不得擅自进入 UIC 校园内进行工程施工，不得开展网络服务业务。

第二章 管理机构与职责

第六条 信息科技服务中心（简称：信息中心）是校园网络基础设施建设、管理和网络信息安全管理的领导机构，负责相关工作的领导、组织、协调和重大问题的决策。

第七条 信息中心-网络组是校园网基础设施建设和管理工作的执行部门，负责校园网规划、技术论证和审核；负责校园网具体实施、组织协调；负责在通讯基础

设施的建设和管理中与运营商的对接；负责校园网的日常管理、运行维护、咨询培训和用户服务等工作。

第三章 基础设施建设管理

第八条 在校区内新建、改造、装修办公室和教室等场所，凡涉及到校园网基础设施变更的项目，各单位应在立项阶段向信息中心提出建设申请。信息中心将依据学校信息化总体规划和具体情况提出建设方案、施工标准和指导意见。对于自行布线施工安装的网络，信息中心将视其为自建网络，不予接入校园网。对因施工造成原有网络设备、线缆损坏和对现有网络产生干扰和影响的，将追究相应责任并要求限期整改。任何单位和个人，未经信息中心同意，不得擅自安装、拆卸或改变网络设备。

第九条 信息中心-网络组负责全校光纤网络的建设和管理。校园内公共区域无线网络（WLAN）由信息中心统一建设，原则上只建设一套无线网络接入系统，通过设置多个无线网络服务集标识（SSID）向校内师生和校外访客提供用户验证接入。

第十条 根据学校师生通讯业务的需要，运营商在校园范围内建设传输线路、通信机房和基站等通讯基础设施的，须向信息中心提交需求报告和设计方案。信息中心会同有关单位进行技术论证和审核，并由学校审批相关场所、签订场地合同后方可进行施工建设，正式投入使用后，由后勤保障部进行日常物业管理。对于具备共建、共享条件的项目，运营商应结合目前已有的资源进行施工建设。校园通讯设施建成后，由信息中心参与组织验收，验收合格后方可投入使用。

通信基站应符合国家的相关标准，对于不符合标准的已建基站将予以拆除。通信基站在运行过程中，运营商须做好用电安全工作，防止安全事故的发生。

校园内通信基站实施备案管理制度。基站所需的场地学校与运营商签订租赁协议。如需使用校园网相关的基础设施，由信息中心代表学校与运营商签订租赁协议。对于未向学校备案的基站，学校将停止供电并限制场地使用。根据教学、科研需要，学校有权要求运营商对通信基站进行关停和启用。

第十一条 根据互联网的发展情况和师生的上网需求，信息中心应积极探索和应用更优的互联网接入方案，不断提高校园网用户访问互联网的速度和质量。

第四章 用户管理

第十二条 所有校园网用户必须遵守《中华人民共和国网络安全法》、《中华人民共和国计算机信息系统安全保护规定》、《中华人民共和国计算机信息网络国际联网管理暂行规定》和国家其他的有关法律法规。

第十三条 学校实行网络安全责任制。根据《中华人民共和国网络安全法》要求，学校对校园网进行管理、监控，并保留 6 个月用户上网日志。

第十四条 校园网账号限用户本人使用，不得转借、转让或者出售他人使用，因此产生的损失、纠纷等应由用户本人负责。

第十五条 用户在使用校园网过程中遇到的任何问题可以向信息中心反馈、处理。

第十六条 在活动或会议中来宾需要使用校园网 ，应向信息中心提出申请，不得将个人账号提供给来宾使用。

第十五条 严禁校园网络用户进行下列行为：

（一）从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动。

（二）盗用他人网络账号。

（三）私自转借、转让网络账号，造成危害。

（四）制作或提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具。

（五）不按国家和学校有关规定擅自开设代理服务器、宽带路由器、接纳未实名认证的网络用户。

（六）未经信息中心允许，私自提供网络信息服务，包含但不限于 DHCP、FTP、Web、BBS 和网络游戏等。

（七）未经允许，进入计算机信息网络或者使用计算机信息网络资源的。

（八）未经允许，对计算机信息网络功能进行删除、修改或者增加的。

（九）未经允许，对计算机信息网络中存储、处理或者传输的数据和应用程序进行删除、修改或者增加。

（十）利用校园网发布传播危害国家安全、破坏社会稳定等不良信息。

（十一）其他危害计算机信息网络信息安全的。

第十六条 对于影响其他用户正常使用网络的个人电脑或服务器，信息中心将采取断网操作。解决相关问题后，方可恢复其校园网接入。

第十七条 商户如需使用校园网络服务，须由其相应的校内管理部门向信息中心申请。

第五章 网络安全管理

第十八条 严禁在校园网上使用来历不明、引发病毒传染的软件；对于来历不明的可能引起计算机病毒的软件应使用专业杀毒软件检查、杀毒。确属用于教学、实验和研究性质需要使用此类软件的，需报信息中心批准并在实验室场所使用，否则一经定位查实将取缔违反者的校园网使用资格，造成破坏构成违法违纪的移交司法机关按国家有关法律法规处理。

第十九条 校园网主、辅节点设备及服务器等发生安全事件、以及遭到黑客攻击后，校园网负责单位必须立即向学校及公安机关报告。

第二十条 校园网工作人员和用户在网络上发现有碍社会治安和不健康的信息有义务保留记录并及时上报网络管理人员。

第二十一条 严格遵守国家有关信息安全的法律法规，遵守国家信息安全保密管理规定，不得在联网的计算机信息系统中存储、处理和传递各类有害信息。

第二十二条 用户应加强计算机病毒的预防和治理，禁止传播计算机病毒的任何行为，禁止任何形式的网络攻击和网络入侵行为。

第二十三条 未经审批，外来人员不得使用校园网，学校公共计算机一律不准对社会开放。

第二十四条 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。

信息资源保密等级可分为：（1）可向 Internet 公开的；（2）可向校内公开的；（3）可向有关单位或个人公开的；（4）仅限于本单位内使用的；（5）仅限于个人使用的。

第六章 附则

第二十四条 违反本管理规定的，视情节轻重采用以下一种或多种措施进行处理：

（一）限期整改；

（二）关闭使用者账号、IP 或端口；

（三）报学校有关职能部门或当事人所在单位处理；

（四）触犯法律法规的，将移交司法、公安部门处理。

第二十五条 本办法自公布之日起生效，解释权归 UIC 信息科技服务中心。