

## 学习资料 1

# 《中华人民共和国网络安全法》

(2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过 根据2025年10月28日第十四届全国人民代表大会常务委员会第十八次会议《关于修改〈中华人民共和国网络安全法〉的决定》修正)

## 目 录

第一章 总 则

第二章 网络安全支持与促进

第三章 网络运行安全

第一节 一般规定

第二节 关键信息基础设施的运行安全

第四章 网络信息安全

第五章 监测预警与应急处置

第六章 法律责任

第七章 附 则

## 第一章 总 则

**第一条** 为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

**第二条** 在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

**第三条** 网络安全工作坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全，推进网络强国建设。

**第四条** 国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

**第五条** 国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

**第六条** 国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

**第七条** 国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

**第八条** 国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

**第九条** 国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

**第十条** 网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

**第十一条** 建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

**第十二条** 网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

**第十三条** 国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义

制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

**第十四条** 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

**第十五条** 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

## **第二章 网络安全支持与促进**

**第十六条** 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

**第十七条** 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和

服务，保护网络技术知识产权，支持企业、研究机构 and 高等学校等参与国家网络安全技术创新项目。

**第十八条** 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

**第十九条** 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

**第二十条** 国家支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展。

国家支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平。

**第二十一条** 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

**第二十二条** 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

### **第三章 网络运行安全**

#### **第一节 一般规定**

**第二十三条** 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

**第二十四条** 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

**第二十五条** 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

**第二十六条** 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

**第二十七条** 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

**第二十八条** 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

**第二十九条** 任何个人和组织不得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；不得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；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

**第三十条** 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

**第三十一条** 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

**第三十二条** 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

## 第二节 关键信息基础设施的运行安全

**第三十三条** 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

**第三十四条** 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保护工作。

**第三十五条** 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

**第三十六条** 除本法第二十三条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

**第三十七条** 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

**第三十八条** 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

**第三十九条** 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

**第四十条** 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

**第四十一条** 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

## **第四章 网络信息安全**

**第四十二条** 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

网络运营者处理个人信息，应当遵守本法和《中华人民共和国民法典》、《中华人民共和国个人信息保护法》等法律、行政法规的规定。

**第四十三条** 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

**第四十四条** 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

**第四十五条** 个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

**第四十六条** 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

**第四十七条** 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

**第四十八条** 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

**第四十九条** 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

**第五十条** 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

**第五十一条** 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

**第五十二条** 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取删除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

## **第五章 监测预警与应急处置**

**第五十三条** 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

**第五十四条** 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

**第五十五条** 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

**第五十六条** 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

**第五十七条** 发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

**第五十八条** 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

**第五十九条** 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

**第六十条** 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

## **第六章 法律责任**

**第六十一条** 网络运营者不履行本法第二十三条、第二十七条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

关键信息基础设施的运营者不履行本法第三十五条、第三十六条、第三十八条、第四十条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处五万元以上十万元以下罚款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款；造成关键信息

基础设施丧失主要功能等特别严重危害网络安全后果的，处二百万元以上一千万元以下罚款，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

**第六十二条** 违反本法第二十四条第一款、第二款和第五十条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

有前款第一项、第二项行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。

**第六十三条** 违反本法第二十五条规定，销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，由有关主管部门责令停止销售或者提供，给予警告，没收违法所得；没有违法所得或者违法所得不足十万元的，并处二万元以上十万元以下罚款；违法所得十万元以上的，并处违法所得一倍以上五倍以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、

吊销相关业务许可证或者吊销营业执照。法律、行政法规另有规定的，依照其规定。

**第六十四条** 网络运营者违反本法第二十六条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

**第六十五条** 违反本法第二十八条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告，可以处一万元以上十万元以下罚款；拒不改正或者情节严重的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。

**第六十六条** 违反本法第二十九条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收

违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十九条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

**第六十七条** 关键信息基础设施的运营者违反本法第三十七条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令限期改正、停止使用、消除对国家安全的影响，处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

**第六十八条** 违反本法第四十八条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

**第六十九条** 网络运营者违反本法第四十九条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取删除等处置措施、保存有关记录、向有关主管部门报告，或者违反本法第五十二条规定，不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取删除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告、予以通报，可以处五万元以上五十万元以下罚款；拒不改正或者情节严重的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

有前款行为，造成特别严重影响、特别严重后果的，由有关主管部门处二百万元以上一千万元以下罚款，责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第五十条第二款规定的安全管理义务的，依照前两款规定处罚。

**第七十条** 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）拒绝、阻碍有关部门依法实施的监督检查的；

（二）拒不向公安机关、国家安全机关提供技术支持和协助的。

**第七十一条** 有下列行为之一的，依照有关法律、行政法规的规定处理、处罚：

（一）发布或者传输本法第十三条第二款和其他法律、行政法规禁止发布或者传输的信息的；

（二）违反本法第二十四条第三款、第四十三条至第四十五条规定，侵害个人信息权益的；

（三）违反本法第三十九条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。

违反本法第四十六条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关依照有关法律、行政法规的规定处罚。

**第七十二条** 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

**第七十三条** 违反本法规定，但具有《中华人民共和国行政处罚法》规定的从轻、减轻或者不予处罚情形的，依照其规定从轻、减轻或者不予处罚。

**第七十四条** 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

**第七十五条** 网信部门和有关部门违反本法第三十二条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

**第七十六条** 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

**第七十七条** 境外的机构、组织、个人从事危害中华人民共和国网络安全的活动的，依法追究法律责任；造成严重后果的，国务院公安部门 and 有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

## 第七章 附 则

**第七十八条** 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

**第七十九条** 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

**第八十条** 军事网络的安全保护，由中央军事委员会另行规定。

**第八十一条** 本法自 2017 年 6 月 1 日起施行。

# 教育部等九部门关于加快推进 教育数字化的意见

教办〔2025〕3号

为贯彻落实《教育强国建设规划纲要（2024—2035年）》，以教育数字化为重要突破口，开辟教育发展新赛道和塑造发展新优势，全面支撑教育强国建设，提出如下意见。

## 一、总体要求

坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻党的二十大和二十届二中、三中全会及全国教育大会精神，全面落实习近平总书记关于教育的重要论述特别是关于教育数字化的重要指示精神，深入实施国家教育数字化战略，坚持应用导向、治理为基，秉承联结为先、内容为本、合作为要，聚焦集成化、智能化、国际化，扩大优质教育资源受益面，促进人工智能助力教育变革，加快形成泛在可及的终身教育体系，助力建设人人皆学、处处能学、时时可学的学习型社会，为有效应对新一轮科技革命和产业变革、加快建设教育强国提供有力支撑。

工作中要做到：坚持立德树人，牢牢把握正确政治方向和价值导向，提高网络育人能力。坚持应用导向，以深度应用引领教育高质量发展。坚持数字赋能，推动教育理念、教学模式和教育治理整体性变革。坚持以人为本，着力培养学生高阶思维、思考判断能力、实践能力。坚持改革创新，主动顺应人工

智能等新技术发展趋势，健全适应数字化发展的制度体系。坚持统筹规划，试点先行，强化部门协同、央地联动、区域协调，鼓励社会参与。坚持安全发展，筑牢可信可控安全屏障。坚持开放合作，深化国际交流，增强中国数字教育全球影响力。

## 二、深入推进集成化，建强用好国家智慧教育公共服务平台

（一）完善国家智慧教育“四横五纵”平台资源布局。以国家智慧教育公共服务平台（以下简称国家平台）为枢纽，集成各级优质平台、资源、服务，逐步实现入口统一、资源共享、数据融通。围绕基础教育、职业教育、高等教育、终身教育四大领域和德智体美劳五大版块建设汇聚精品资源。鼓励各地各校、行业企业发挥优势开发精品资源。基础教育建设覆盖国家课程教材、适配不同学情的精品课程资源和科学教育、文化艺术资源。高等教育、职业教育建设覆盖各学科的精品数字课程、虚拟仿真实习实践、学位论文与实践成果等资源。增加思政、体育、美育、劳动教育、特殊教育、语言文字等资源供给。建设覆盖家庭教育、社会教育、老年教育、职业能力提升等终身教育资源。提升平台智能化水平，增强平台开放性，创新资源新形态，增强资源交互性，实现个性化智能推荐。完善资源开发、上线、应用、评价和退出全生命周期管理机制。建立资源评价标准，分级分类开展动态评价，完善专家评估和用户反馈机制，实行数字资源收录和收藏证书制度，推进资源精品化、体系化、专业化，构建高质量资源供给生态。

（二）持续升级国家平台公共服务功能。推动“高效办成一件事”，扩大教育公共服务“一网通办”事项。优化招生入

学、考试评价、学籍查询、学历学位认证、教师资格查询、普通话等级证书查询等服务，优化国家大学生就业服务平台，为大学生实习就业和行业企业招聘提供优质服务。优化出国留学全程在线服务，提升便捷性。

（三）推进国家平台全域深度应用。制定工作指南，明确省市县校各级工作重点和推进机制，遵循不同学段特点和规律制定应用策略，提升应用成效。推动各省（区、市）制定整体推进区域教育公平优质发展数字化解决方案，实现省内平台、资源、服务与国家平台互联互通。深入实施“同上一堂好课”、慕课西部行 2.0 计划、读书行动等，倾斜支持农村地区、民族地区、脱贫地区。推进“专递课堂”“名师课堂”“名校网络课堂”常态化应用，拓展备课授课、作业管理、班级管理、考核评价、家校沟通、课后服务等高频场景应用。深化名师线上工作室等建设，完善在线教研机制。

（四）推进教育数据集成和有效治理。建好国家教育大数据中心，统一数据标准和接口标准，建设跨层级、跨地域、跨部门教育数据共享网络，畅通数据循环。推动教育与国家人口、空间地理、经济社会、行业产业等数据互联互通。加强数据集成，打通学校、学生、教师全链条管理信息系统，逐步实现“一数一源”，深挖教育数据富矿，构建大数据赋能教育治理新体系。

（五）加快构建终身学习公共服务体系。加强学习型社会数字基础设施建设，推动构建泛在可及的终身教育体系。加快出台资历框架标准，建设国家学分银行，促进学历教育和非学历教育纵横贯通。加快建立学习成果认证机制，探索建立基于

学分制的终身学习学历学位授予机制。建好国家智慧教育平台终身教育板块。加快建设新形态国家数字大学，探索线上非学历、学历教育学分认证及学历学位授予新机制。完善国家开放大学体系，建好国家老年大学。

### 三、全面推进智能化，促进人工智能助力教育变革

（六）加强人工智能等前瞻布局。加快建设人工智能教育大模型。完善教育领域多模态语料库，构建高质量自主可控数据集。强化算法安全评估，确保正确价值导向。布局一批前瞻性研究课题，有序开展人工智能应用试点，探索“人工智能+教育”应用场景新范式，推动大模型与教育教学深度融合。推动思政、科学教育、美育、心理健康等领域及数学、物理等基础学科专题大模型垂直应用，培育应用生态。

（七）推动学科专业数字化升级和科研范式变革。面向数字经济和未来产业发展，优化高等教育学科专业设置，超前布局数字领域学科专业，一体化推进人才培养、科技创新、技术研发和成果转化。面向先进制造业和现代服务业数字转型需要，动态调整职业教育专业，赋能产教深度融合，服务“一体两翼”建设和高技能人才培养。以人工智能技术推动科研范式变革，提高科研组织效率，提高成果转化效率，衍生学科增长点，助力建设一批新兴学科、交叉学科。

（八）推动课程、教材、教学数字化变革。完善知识图谱，构建能力图谱，深化教育大模型应用，推动课程体系、教材体系、教学体系智能化升级，将人工智能技术融入教育教学全要素全过程，推动科技教育和人文教育融合。统筹推进大中小学人工智能教育一体化，建设“通用+特色”高校人工智能通识

课程，建设一批高校智慧课程，开好中小学信息科技相关课程，鼓励开设人工智能特色课程。制定数字教材建设和管理指导意见，分领域分专业研发一批示范性精品数字教材，支持地方、学校和企业开发数字教材。探索建设云端学校、智造空间、未来学习中心，建设“人工智能+X”国家级实验教学中心，构建新型教学组织形态，促进学习方式变革。构建“一站式”数智学生社区。通过智能学伴、数字导师等探索人机协同教学新模式，实现人工智能驱动的大规模因材施教，提高教育教学效率和质量。

（九）以师生为重点提升全民数字素养与技能。深入实施提升全民数字素养与技能行动纲要，提升网络文明素养、数字道德伦理。制定完善师生数字素养标准和人工智能应用指引，开展素养提升实践活动和调查评估，提升数字素养与人工智能应用水平。建立大中小学衔接的数字素养培育体系，将数字素养纳入综合素质评价。深化人工智能助推教师队伍建设行动，将数字素养融入教师教育课程体系。建立轮训制度，提高教育管理干部、学校管理者数字素养。

（十）全面支持教育决策和治理。加快建设“教育数字地图”，支持开展趋势预测、规划决策、风险预警。建设基础教育学位预测预警模型，支持优化教育资源布局。建设国家人才供需对接大数据平台，支持动态调整优化专业布局、学科设置和招生规模，促进毕业生高质量充分就业。建设全国学科大数据信息资源库，建立基于大数据的学科发展监测体系。提高教育财务数字化信息化管理能力，加强教育经费使用监管。

（十一）赋能教育评价改革。建立基于大数据和人工智能支持的教育评价机制，面向学校、教师、学生等不同主体，完善结果评价，开展多维度的过程评价、增值评价和综合评价。推动实现教学全过程、发展全要素伴随式数据采集，开展精准画像。强化全面发展育人导向，推进数字化赋能考试评价改革。推进高等教育自学考试等考试的数字化试点。实现高校教学、科研、管理、服务数据共享，推动院校、学科、专业评估数字化转型。

#### 四、大力推进国际化，持续增强数字教育国际影响力

（十二）推动数字教育资源国际共建共享。搭建多边、多层级的数字教育国际合作对话机制，构建数字教育国际合作体系。建好国家平台国际版，丰富国际课程资源，加强与有关国家和国际组织平台对接，探索设立国别专区。持续实施“慕课出海”行动，推动与国外知名高校共建高水平课程。赋能“鲁班工坊”等职教出海项目建设，依托职教海外办学机构、高校海外学习中心、企业海外培训中心等为发展中国家培养“数字+技能”复合型人才。丰富中文数字学习资源，建好中文联盟，提升国际中文教育覆盖面。

（十三）打造具有全球影响力的数字教育品牌。持续办好世界数字教育大会、世界慕课与在线教育大会、国际人工智能与教育会议，建好用好世界数字教育联盟、世界慕课与在线教育联盟。办好数字教育国际期刊，遴选数字教育全球示范案例，定期发布中国智慧教育蓝皮书、全球数字教育发展报告及指数、世界高等教育数字化发展报告及指数，推动形成教育数字化转型发展的世界样板。

（十四）赋能人才国际化培养。合作共建数字课程、数字实训基地与虚拟实验室，推进人才国际化联合培养，加强开放科学和技术合作。建立数字学习学分互认机制，依托国家数字大学与国外高校开展数字学历互认试点，探索人才培养新路径。建好数字教育海外学习中心，重点支持面向发展中国家开展数字技术能力培训。共建教育数字化国际智库，培养国际智库人才。

（十五）积极参与全球数字教育治理。主动参与数字教育相关国际组织，积极与联合国教科文组织、经济合作与发展组织、二十国集团、金砖国家、上海合作组织等合作，推动建立国际数字教育发展共同体。积极参与数字教育国际议程、规则、标准制定，推动国家智慧教育平台、师生数字素养、数字教育安全伦理等方面标准成为国际共识。

## 五、健全教育数字化保障体系

（十六）完善基础设施。积极运用“两新”等国家支持政策，升级教育数字化基础设施。推动公共网络、算力和云资源向教育应用倾斜。建立区域、高校算力资源共享机制。推进智慧校园标准化建设，逐步普及教学智能终端。推进 IPv6 规模部署及应用，推动中小学校合理扩容出口带宽，满足教育需求。引导学校支持网络基础设施建设，逐步实现校园无线网覆盖。加快建设教育专网，探索建设教育行业云，有序推动教育应用上云。

（十七）健全标准规范体系。加快推进教育数字化标准制修订，形成覆盖数字教育软硬件环境、平台工具、数字资源、教育数据、网络安全等方面标准规范。加强教育平台对中文编

码字符集强制性国家标准的支持。制定平台管理、支持服务质量保障标准。推动国家、地方、行业、企业、团体有关教育数字化标准的有机衔接。

（十八）建立多元投入机制。坚持公益性原则，发挥政府主导作用，建立政府、社会、企业共同参与的多元投入机制。做好教育新型基础设施建设、购买优质数字资源和服务等经费保障，对农村、边远地区视情给予倾斜支持。基础电信企业对各级各类学校的网络使用资费给予优惠。统筹利用市场融资等多种渠道，引导社会资本支持教育数字化发展。学校加强经费统筹，保障教育数字化支出。构建全国统一的数字教育资源供给大市场，引导企业研发符合应用需求的数字化教育产品和解决方案，保护资源贡献者知识产权。

（十九）建立应用评价激励机制。坚持以应用为导向，分级分类开展教育数字化建设应用成效评价，纳入学校办学水平评估。在国家教学成果奖等设立数字教育项目，将数字化应用作为申请国家有关教育教学奖项的前置条件，纳入学校和教师评优评先内容。发布国家教育数字化年度报告。

## **六、筑牢教育数字化安全屏障**

（二十）保障重点平台高质量运行。提升关键信息基础设施、平台体系保障能力。严格资源内容审核制度，落实平台主体责任，坚持提供必审、上线必审、更新必审、审必到位原则，确保政治性、导向性、科学性、适用性、规范性、时效性、公益性。构建多部门协同的重点时期保障机制，定期组织开展安全评估和检测。

（二十一）构建网络安全防护体系。依托国家网络身份认证公共服务，建立教育领域身份和数据可信体系，强化实名管理。全面落实教育数据全生命周期安全防护，强化核心和重要数据防篡改、防泄露、防滥用能力。加强未成年人个人信息保护，组织开展个人信息保护合规审计。全面落实网络安全责任制，做好网络安全等级保护。

（二十二）强化人工智能安全保障。建立“人工智能+教育”安全保障制度。落实人工智能算法与大模型备案机制，探索建立算法安全评估制度，有效规避网络攻击、信息茧房、算法霸权、依赖成瘾等问题。坚持以人为本、智能向善的数字伦理准则，加强对智能教育产品、工具、服务监管，规范人工智能应用进校园管理。

## 七、加强组织实施

健全教育数字化领导体系、运维机制和评价机制。建立跨部门协调机制，教育部门负责制定总体方案，具体推进实施；网信、公安部门负责加强教育数字化领域意识形态和网络安全、数据安全、个人信息保护监管及信息技术发展应用，打造健康向上网络环境；发展改革、财政部门负责对教育数字化项目和经费予以支持；科技部门负责加强重点领域科研布局，以人工智能技术推进科研范式变革；工业和信息化、数据管理部门负责推动教育数字化基础设施建设、数据互联互通；人力资源社会保障部门负责制定国家资历框架，协同推进终身教育体系建设。各地各校把教育数字化作为一把手工程，省级教育部门加强统筹实施，抓好系统培训和领导力培训，提升认知能力和执行能力，结合实际制定实施方案，大胆试点，积极开发个性资

源，推进创新应用，探索教育数字化助推教育公平优质发展新路径和教育教学新方法、人才培养新模式。建好教育数字化专家咨询委员会，加强研究和指导。建设高素质专业化教育数字化管理和技术支持队伍。宣传推广各地各校有效做法和经验。

教育部 中央网信办 国家发展改革委  
科技部 工业和信息化部 公安部 财政部  
人力资源社会保障部 国家数据局  
2025 年 4 月 11 日

### 学习资料 3:

## 纪录片《教育家精神》

中央广播电视总台联合教育部推出六集纪录片《教育家精神》，该纪录片以十八大以来习近平总书记关于教育的重要论述，特别是关于大力弘扬教育家精神的重要指示批示精神为指导，以中国近现代和当代各个历史时期内教育界的重大事件为时代背景，紧紧围绕教育家精神的内涵，深入挖掘中华传统师道精神，讲述和呈现了著名教育家和优秀教师胸怀天下、兴教强国、治学弘道、教书育人的感人故事和师德风范。请广大教职工积极开展学习、涵养高尚师德，视频链接如下：

### 1. 《心有大我 至诚报国》

<https://tv.cctv.com/2024/09/04/VIDEYa6mnXR0kiouN8MW1E6B240904.shtml?spm=C52507945305.Pknrmn9ZARZj.0.0&from=guanwangsj> )

### 2. 《言为士则 行为世范》

<https://tv.cctv.com/2024/09/05/VIDEQMqq06jFKF6tTtJAb9i4240905.shtml?spm=C52507945305.Pknrmn9ZARZj.0.0&from=guanwangsj>

3. 《启智润心 因材施教》

<https://tv.cctv.com/2024/09/06/VIDEvKWMbRvL7YJzyzhkW6Ze240906.shtml?spm=C52507945305.Pknrmn9ZARZj.0.0&from=guanwangsj>

4. 《勤学笃行 求是创新》

<https://tv.cctv.com/2024/09/09/VIDEvkd0u8eyKrHgd8m0k56M240909.shtml?spm=C52507945305.Pknrmn9ZARZj.0.0&from=guanwangsj>

5. 《乐教爱生 甘于奉献》

<https://tv.cctv.com/2024/09/10/VIDE2zXm6C8XRXxUjnM0auB240910.shtml?spm=C52507945305.Pknrmn9ZARZj.0.0&from=guanwangsj>

6. 《胸怀天下 以文化人》

<https://tv.cctv.com/2024/09/11/VIDE2u7rqYsh3sLP887zrJKg240911.shtml?spm=C52507945305.Pknrmn9ZARZj.0.0&from=guanwangsj>

学习资料 4:

## 教师师德失范警示教育案例汇编

### （坚守廉洁自律篇）

教师应坚守廉洁自律。严于律己，清廉从教；不得索要、收受学生及家长财物，不得参加由学生及家长付费的宴请、旅游、娱乐休闲等活动，或利用家长资源谋取私利。

1. **湖南文理学院教师刘某某私自收取并侵占学生费用问题。**刘某某利用担任文史与法学学院学工办副主任、辅导员、班主任等的便利，通过支付宝和微信转账方式，私自收取并侵占该校学生学杂费和班费共计 77 万余元。学校将刘某某案件移送公安机关立案侦查，公安机关对刘某某执行刑事拘留。刘某某的行为违反了《新时代高校教师职业行为十项准则》第二、第九项规定。根据《中国共产党纪律处分条例》《教育部关于高校教师师德失范行为处理的指导意见》，给刘某某开除党籍、免职等处分，根据司法机关对其涉嫌犯罪问题的处理结论，依法依规给予进一步处理。

2. **宁夏大学教师马某某违规获取津贴问题。**2019 年 9 月至 2022 年 5 月，马某某擅自给他人发放津贴、违规领取管理绩效和教学工作量津贴。马某某的行为违反了《新时代高校教师职业行为十项准则》第九项规定。根据《中国共产党纪律处分条例》《事业单位工作人员处分暂行规定》《教育部关于高校教师师德失范行为处理的指导意见》等相关规定，给予马某某党内严重警告处分，给予其政务降级、专业技术岗位等级由三级降至四级等处分，对其违规滥发和超标准领取的津贴予以悉数上缴。对所在学院党总支书记进行诫勉谈话。

3. **吉林农业科技学院教师王某某性骚扰学生、学术不端等问题。**2018 年 10 月，王某某违规参加由学生支付费用的宴请和娱乐活动期间存在性骚扰学生行为，且存在论文抄袭造假情况。王某某的行为违反了《新时代高校教师职业行为十项准则》第六项、第七项、第九项规定。根据《事业单位工作人员处分暂行规定》《教育部关于高校教师师德失范行为处理的

指导意见》等相关规定，给予王某某开除处分，撤销其教师资格，收缴教师资格证书，将其列入教师资格限制库。学校党委对其所在学院党总支书记和院长给予党内警告处分。

4. 湖南科技大学工作人员刘俊在研究生论文送审中向学生索要现金，受到党内严重警告、行政记过处分。湖南科技大学马克思主义学院工作人员刘俊在办理 2017 年下半年研究生毕业论文送审等工作中，向学生索要现金 9100 元，收取学生论文打印费及聚餐费用 1450 元，涉及金额共计 10750 元。