北京师范大学智慧学习研究院
Smart Learning Institute of Beijing Normal University

在线学习中的个人数据和隐私保护

面向学生、老师和家长的指导手册

2020年6月 1.0版

出版单位：北京师范大学智慧学习研究院
合作单位：联合国教科文组织教育信息技术研究所
联合国教科文组织国际农村教育研究与培训中心

在线学习中的个人数据和隐私保护：面向学生、教师和家长的指导手册

Rights and Permissions

引用信息：

Huang, R.H., Liu, D.J.，(2020). Personal Data and Privacy Protection in Online Learning: Guidance for Students, Teachers and Parents. Beijing: Smart Learning Institute of Beijing Normal University.

黄荣怀，刘德建，朱立新，陈虹宇，杨俊锋， Ahmed Tlili，方海光，王绍峰等 (2020). 在线学习中的个人数据和隐私保护：面向学生、教师和家长的指导手册 . 北京：北京师范大学智慧学习研究院 .

2020 年 6 月　1.0 版

在线学习中的个人数据和隐私保护：
面向学生、老师和家长的指导手册

2020 年 6 月　1.0 版

前言

新冠肺炎疫情给我们的安全、健康和教育带来了前所未有的挑战。联合国教科文组织于 4 月 5 日公布的数据显示，全球有 15.9 亿学生无法重返校园，占全球学生总数的 91.3%。之后，疫情对教育的影响逐渐减弱。截至 6 月 13 日，依然有 11.1 亿学生无法回到校园，占在校学生总数的 63.3%。在这种特殊的情况下，很多学生不得不进行在线学习，伴随着大量的个人数据被共享，也暴露出个人数据的安全隐患。个人数据和隐私保护从未像今天这样急迫，其已被联合国教科文组织列为我们面临的最大挑战之一。如何保护在线学习中的个人数据和隐私，成为学生、教师和家长共同面临的一个重要问题。

在线学习过程中，个人数据是通过学生 / 教师与工具或平台的互动而产生的。隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。隐私策略是一种声明或法律文件 (在隐私法中)，它公开了一方收集、使用、披露和管理客户或客户数据的部分或全部方式。随着在线学习的大规模应用，个人隐私保护已成为在线学习面临的一个关键问题。许多国家和组织制定了有关个人数据保护的法律、法规和政策文件。日本、英国、澳大利亚等国家、联合国 (UN)、经济合作与发展组织 (OECD)、亚太经济合作组织 (APEC)、国际标准化组织 (ISO) 等组织也相继颁布了一系列保护个人数据的法律、规章、框架和原则。

近日，联合国教科文组织教育信息技术研究所 (UNESCO IITE) 与清华大学研究团队合作，起草了针对在线教育平台的个人数据安全技术指南。该技术指南就技术解决方案、管理以及提高认识等方面向在线教育平台提供者、相关教育和技术管理人员提出宝贵建议。我们的这本指导手册旨在指导学生、老师和家长于在线学习中保护个人数据和隐私。

本指导手册梳理了在线学习中个人数据安全风险，并从学习前、学习中、学习后三个方面提出了个人数据保护的具体策略。手册阐述了如何保护在线学习个人数据的基本思路，并就具体的学习活动对学习者进行具体指导，力求使在线学习环境成为一个智能的个人数据保护环境。

我们谨代表联合国教科文组织 IITE 和联合国教科文组织 INRULED 向来自全球的合作伙伴表示感谢。我们要特别感谢中华人民共和国教科文组织全国委员会对本手册的大力支持。感谢联合国教科文组织 INRULED、IITE、ICHEI 的专家们。感谢智慧学习环境国际协会 (IASLE)，阿拉伯教科文组织 (ALECSO) 和 Edmodo 在手册研制期间的反馈和意见。感谢众多国际合作伙伴、研究人员和工作人员为这本手册的内容开发和网络研讨会组织所作出的努力。

致谢

本手册的研制和发布得到了许多人的帮助。我们非常感谢他们为完成手册而投入的长时间艰苦的工作。没有他们的协助，这本手册是不可能完成的。

我们要特别感谢 Svetlana Knyazeva，Denis Kapelyushnik，张定文，郤红艳，邓睦申，刘佳佳，汪时冲，宿金超，何竑瑾，赵睿恒，潘柳霞，张鹏等项目成员的帮助。我们还要感谢多个国际合作伙伴、研究人员和工作人员的贡献，他们在网络研讨会上为本指南提供了新的想法。

感谢来自联合国教科文组织农村教育国际研究和培训中心、联合国教科文组织信息技术教育研究所、联合国教科文组织国际高等教育创新中心、国际智慧学习环境协会、阿拉伯教科文组织以及 Edmodo 的专家，感谢他们在编写本指南期间提供的专业意见。

目录

摘要 1

第一章 在线数据安全和隐私保护刻不容缓 2

1.1 在线学习和个人数据 2

1.2 学生的个人数据保护 4

1.3 个人数据保护的法律法规 6

第二章 在线学习中的个人数据和隐私 10

2.1 个人数据 10

2.2 学生数据和隐私 17

2.3 隐私保护框架 21

2.4 在线学习数据收集 24

2.5 个人对数据的权力 25

第三章 个人设备设置和学习工具选择 27

3.1 设置个人设备 27

3.2 管理网络连接 28

3.3 选择和安装学习工具 30

3.4 浏览隐私政策 32

第四章 注册和登录时的隐私安全 35

4.1 创建账户的密码策略 35

4.2 公共设备的安全问题 39

第五章 在线学习平台中的数据和隐私安全 42

5.1 课程注册与管理 43

5.2 个性化学习服务 45

5.3 使用搜索服务 46

5.4 管理定位服务 48

5.5 备份个人数据 49

第六章 社交网络工具中的数据和隐私保护 52

6.1 使用视频会议工具 52

6.2 发布网络信息内容 55

6.3 屏蔽不健康内容 56

第七章 个人信息删除 66

7.1 删除在线学习数据 66

7.2 注销账户 69

结语 74

参考文献 76

术语表 82

主题索引 84

摘要

随着新型冠状病毒肺炎的蔓延，许多学生不得不在网上学习。事实上，在线学习正逐渐成为终身学习的一个标志。因此，如何在在线学习中保护个人数据和隐私成为学生、家长和管理者关注的重要问题。为了保护在线数据及隐私，学生应了解在线学习中的个人数据是如何产生的，以及如何保护在线个人隐私。

手册中针对在线学习中的个人数据和隐私保护问题提出了一些建议。

第一章介绍了在线学习的概念、典型的学习活动，以及学习过程中产生的个人数据。同时，也介绍了个人数据保护的法律法规、政策，尤其是儿童个人数据保护相关的的法律法规和政策。在线学习过程中，如何保护自己的个人数据是学生们迫切需要解决的问题。

第二章详细阐述了个人数据和隐私的定义和构成，特别是在线个人数据的生命周期以及学生数据和隐私的特征。同时也梳理了国内外有关隐私保护的框架和原则。此外，还讨论了在线学习中收集的数据以及学生和家长关于这些数据的权利。

第三章至第七章介绍了保护在线数据的具体操作建议。其中，第三章讨论了在线学习前的准备工作，如设置个人数字设备和网络、选择和安装在线学习工具等。第四章主要讨论了注册和登录在线学习平台时如何保护个人数据。第五章对于在线学习者保护个人隐私至关重要，它重新梳理了在线学习中的一系列活动，包括加入课程，使用个性化学习服务、定位服务，以及备份学习数据等。第六章主要介绍了利用社交工具学习时应注意保护自己和他人的数据和隐私，如浏览网络、使用网络会议系统、论坛发帖等。第七章介绍了完成在线学习后如何清理在线个人数据。

手册旨在提出如何保护在线学习的个人数据的基本思想，并就具体的学习活动为学习者提供具体的指导。让我们共同努力，让学习环境变成更加智能的个人数据保护环境。

第一章 在线数据安全和隐私保护刻不容缓

1.1 在线学习和个人数据

在线学习

在线学习是指在同步或异步环境中使用不同设备 (手机、笔记本电脑等) 与互联网连接的学习体验。在这些环境中，学习者可以在任何地方（独立）学习，并与教师和其他学习者互动（Singh & Thurman，2019 年）。

在线学习中，学生、教师和知识之间的互动关系已经被诸多理论所解读。Terry Anderson 的在线学习模型 (2011) 阐明了这三个要素之间的相互作用，可以帮助我们加深对复杂教育环境的理解。

在老师的帮助下，学生可以通过各种基于互联网的同步和异步活动（视频、音频、网络会议、聊天或虚拟世界交互）自主决定学习的进度、指导和评价。这些同步和异步的在线学习环境可以促进学生的社交和协作技能以及人际关系的发展。

学生也可以直接与多种格式的学习资源进行交互。在线学习模型说明了结构化学习工具（模拟、游戏、虚拟实验室等）和自主学习的关系。我们可以看到，学生不是孤立的，他们身边或网络上的学习伙伴、正式和非正式的学习团体、以及父母都可以为自主学习提供重要支持（波特，1998）。

(1) 在线学习工具的类别

有效选择和使用学习工具将有益于学生查找、获取和处理信息，交流协作，建构知识，以具体的方法组织并表述理解和评价学习效果。学习工具的选择要考虑工具的便捷性，即工具要能帮助教师方便快捷地制作和管理资源、发布通知和管理学生；帮助学生方便快捷地获取资源、参与学习活动；帮助师生和学生之间方便快捷地实时互动交流；帮助教师、家长、学校及时了解学生的学习动态和家校互通。

为方便各级各类学校的教师快速方便地选择各种学习工具，支持在线教学的顺利开展，这里按照工具对教学过程中各个环节、不同活动的支持作用将学习工具划分为八大类：

- 资源制作工具，包括 PPT 录制软件、屏幕截图软件、视频制作软件、多媒体资源制作软件等；
- 同步教学工具，包括交互式教学软件，远程办公软件和在线课程平台；
- 异步教学工具，包括国家、区域、高校和企业推出的各种在线教学平台；
- 自主学习工具，包括所有学科的学习类 App；
- 知识建构的工具，包括认知工具、协同编辑工具、虚拟仿真工具等；
- 学情分析工具，包括数据分析的 App、网站和课堂互动软件；
- 练习与测评工具，包括各种适合练习和测评的工具；
- 资源和课堂管理工具，包括各种学习资源丰富、学生人数较多和学习任务较多的在线教学组织管理工具。

(2) 在线学习的典型步骤

分析在线学习中的数据保护，需要考虑使用多种在线学习工具的典型步骤。

1) 个人设备设置和学习工具选择

在线学习之前，设备、网络、工具的准备，以及隐私政策的阅读是个人数据保护的前提。

- 设置个人设备
- 管理网络连接
- 选择和安装学习工具
- 浏览隐私政策

2) 注册和登录时的隐私安全

登录任何一个学习平台时，往往需要在平台上进行注册，但是用户常忽视注册操作，导致个人信息泄露等问题。

- 创建账户密码策略
- 安全使用公共设备

3) 在线学习平台中的数据和隐私安全

注册学习平台后，学习者可以报名参加课程，在论坛、博客上发布信息，浏览和学习课程内容，这些环节都涉及到个人数据保护的问题。

- 课程注册与管理
- 个性化学习服务
- 使用搜索服务
- 管理定位服务
- 备份个人数据

4) 社交网络工具中的数据和隐私保护

社交网络正越来越多地用于在线学习。它提供了一种媒介，使学生能够积极主动地进行多人协作，并与老师和同学共同创造知识、分享经验。然而，社交网络的过度使用可能会对学生的学习产生负面影响，如个人信息泄露、注意力分散、过度沉迷网络等。使用社交网络进行学习时应该在以下几方面加以注意：

- 使用视频会议工具
- 发布网络信息内容
- 屏蔽不健康内容

5) 个人信息删除

完成在线学习后，学习者应注意学习过程中生成的数据，并决定是否删除这些数据。如果决定删除数据，可以参考如下建议和方法：

- 删除在线学习数据
- 注销账户

1.2 学生的个人数据保护

在线学习过程中，数据是通过学生 / 教师与工具或平台之间的互动产生的。在大多数情况下，学生 / 教师可能没有保护个人数据的意识。随着互联网与教育的融合不断加深，用户必须具备基本的数字素养，尤其是个人数据和隐私保护。

隐私和个人数据保护是紧密相连的。在收集、存储或使用数据的任何地方，都会出现隐私问题。隐私的核心是授权访问——谁拥有它，谁定义它。个人数据保护的重点是数据的使用和管理，例如政策制定应确保用户的个人信息以适当的方式被收集、共享和使用。

David Flaherty (1989) 认为网络计算机数据库对隐私构成了威胁。他将“数据保护”作为隐私的一个方面，涉及“个人信息的收集、使用和传播”。这一概念形成了各国采用的信息保护实践基础。

许多国家和组织制定了与个人数据保护有关的法律、法规和政策文件（如表 1-1 所示），对学生和儿童采取了特别保护措施。

在针对不同群体的隐私保护中，学生群体应该重点关注。一方面，由于教育的需要，学生在学习过程中会产生大量的个人信息，如姓名、住址、家庭住址、考试成绩、学习行为等。另一方面，为了便于管理，学校收集了大量学生的个人信息。如果这些信息得不到保护，就很容易泄露和被非法使用。

然而，专门针对学生隐私保护的立法较少，通常只是一般法规中的少数条款。一些组织和学校基于本国的法律法规，制定了专门条例和指导方针，帮助家长和教师保护学生数据。

表 1-1 关于学生和儿童个人信息保护的法律法规

法律法规	国家或组织	发布日期	年龄范畴	概要
儿童在线隐私和言论自由 (Children’ s Online Privacy and Freedom of Expression)	联合国儿童基金会 (United Nations International Children's Emergency Fund, UNICEF)	2018	18 岁以下	联合国儿童基金会和国际电信联盟 (International Telecommunications Union, ITU) 于 2015 年出版的《儿童在线保护行业准则》(The Guidelines for Industry on Child Online Protection) 探讨了企业在数字世界中应尊重儿童权利。该工具包以相关准则为基础，增加了儿童隐私权和言论自由的内容。
部长委员会关于在数字环境中尊重、保护和实现儿童权利的准则的 cm / rec (2018)7 号建议 (Recommendation CM/Rec(2018)7 of the Committee of Ministers to member States on Guidelines to respect, protect and fulfil the rights of the child in the digital environment)	欧洲委员会 (Council of Europe)	2018	18 岁以下	儿童有权在数字环境中享有私人和家庭生活，其中包括保护其个人数据和尊重其私人通信的保密性。各成员国必须尊重、保护和确保儿童的隐私权和数据保护权力。各成员国应确保利益相关方，特别是处理个人数据的利益相关方，以及儿童的同伴、父母或监护人，教育工作者了解并尊重儿童的隐私权和数据保护权力。
K-12 网络安全法案 K-12 Cybersecurity Act	美国	2019	从幼儿园到 12 年级	《K-12 网络安全法案》指导美国国土安全部 (DHS) 检查学校在网络安全方面面临的风险和挑战，从而帮助其加强其网络安全。
儿童个人信息网络保护规定 Provisions on the Cyber Protection of Children's Personal Information	中国	2019	14 岁以下	任何组织和个人不得制作、发布、传播侵害儿童个人信息安全的信息。

扩展阅读

谷歌将因儿童隐私问题支付 1.7 亿美元罚款

美国政府 2019 年 9 月 4 日宣布与谷歌公司及其子公司 YouTube 达成和解协议，后者将支付 1.7 亿美元罚款，此前 YouTube 公司被控未经父母准许非法收集儿童个人信息并用于推送广告盈利。

美联邦贸易委员会 4 日在一份新闻公报中说，根据和解协议要求，谷歌和 YouTube 将因违反《儿童在线隐私保护法》向美联邦贸易委员会和纽约州分别支付 1.36 亿美元和 3400 万美元。这是该法案 1998 年通过以来，美联邦贸易委员会就侵犯儿童隐私问题开出的最大罚单。

这也是美国政府近两个月来第二次就用户隐私向美国科技公司开出大额罚单。7 月 24 日，美联邦贸易委员会宣布同意与脸书公司就保护用户隐私达成和解协议，内容包括脸书赔付 50 亿美元罚款，并接受美联邦贸易委员会的进一步监管。

纽约州首席检察官利蒂希娅 · 詹姆斯在一份声明中说，谷歌和 YouTube 明知非法仍监控、跟踪儿童并向他们精准推送广告，赚取大量广告收入，这种对权力的滥用将儿童置于危险中。

1.3 个人数据保护的法律法规

随着信息技术的发展和互联网的普及，越来越多的国家和组织制定了个人数据保护相关的法律、法规和政策文件，如表 1-2 所示。社会组织和企业也已采取措施，以确保个人资料的安全。

一般来说，保护个人信息安全的法律往往体现在各国的法律中。这些法律将一般性原则（如跨国数据保护原则）转化为某一国家的具体法律制度。而国际性的相关法规的核心往往是原则性的，比如美国联邦贸易委员会提出的旨在保护在线隐私的公平信息原则（Fair Information Privacy Principles）。

欧盟

《欧洲人权公约》(The European Convention on Human Rights) 和《欧洲联盟基本权利宪章》第 8 条 (Article 8 of the Charter of Fundamental Rights of the European Union) 明确了个人信息保护的基本权利。2018 年，欧盟颁布了世界上最严格的个人信息保护法—《通用数据保护条例》(General Data Protection Regulation，GDPR)，规定了企业如何收集，使用和处理欧盟公民的个人数据。

美国

继 1974 年颁布《隐私法》之后，美国在金融领域、消费者和儿童保护等方面颁布了若干法律，如《儿童在线隐私保护法》(The Children’ s Online Privacy Protection Act，COPPA)、《K-12 网络安全法》(K-12 Cybersecurity Act of 2019) 等。

中国

中国于 1997 年 12 月颁布了《互联网计算机信息网络安全保护管理办法》，加强计算机信息网络的安全保护。2017 年，《网络安全法》实施，规定了网络信息安全法的总体目标和基本原则。2019 年出台的《儿童个人信息网络保护规定》，标志着中国在加强互联网安全、保护个人隐私（特别是儿童隐私方面）迈出了新的一步。

其他国家和国际组织

日本、英国、澳大利亚、巴西、南非等国家，联合国（UN）、经济合作与发展组织 (OECD)、亚太经合组织 (APEC)、国际标准化组织 (ISO) 等也发布了个人数据保护相关的法律、法规、框架和原则等。

表 1-2：各国家和国际组织的法律法规

法律法规	国家或组织	发布日期	概要
数字时代的隐私权 (68/167. The Right to Privacy in the Digital Age)	联合国 (United Nations，UN)	2013	重申人们线上和线下的权利都要得到保护，呼吁各成员国尊重和保护数字通信中的隐私权。
第 16 号一般性意见第 17 条 (General Comment No. 16 Article 17)	联合国人权事务委员会 (United Nations' Human Rights Committee, UNHRC))	1988	尊重隐私、家庭、住宅和通信的权利，以及荣誉和名誉的保护。
保护隐私及个人数据跨境流动指引 (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)	经济合作与发展组织（Organization for Economic Co-operation and Development, OECD）	1980	自动数据处理技术的发展使大量数据能够在几秒钟内跨国界、甚至跨大洲传输，有必要考虑个人数据的隐私保护。
教育领导人、教育工作者和学生的标准 (ISTE Standards for Education Leaders, Educators, and Students)	国际教育技术学会（The International Society for Technology in Education，ISTE）	1998	ISTE 标准帮助各国教师和教育管理者为学习者在工作和生活中做好充分准备。

法律法规	国家或组织	发布日期	概要
个人识别信息保密性保护指南 (NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII))	美国商务部国家标准与技术研究院 (The National Institute of Standards and Technology，NIST)	2010	本文件旨在协助联邦机构保护信息系统中个人信息 (PII) 的机密性。本文件解释了在信息安全的背景下保护 PII 机密性的重要性，并使用公平信息处理原则（Fair Information Privacy Principles）解释了其与隐私的关系。该原则是大多数隐私法律和隐私最佳实践的基本原则。应保护 PII，防止不适当的访问、使用和披露。
ISO/IEC 29100:2011 国际标准	国际标准化组织 (International Organization for Standardization，ISO)	2011	该国际标准为信息和通信技术 (ICT) 系统中的个人信息 (PII) 保护提供了一个高级框架。
一般数据保护条例 (General Data Protection Regulation, GDPR)	欧盟	2018	让个人对其个人数据拥有控制权，并通过统一欧盟内部的负责，简化国际业务的监管环境。
隐私法 (The Privacy Act)	美国	1974	本法律制定了一套公平信息处理规范 (Code of Fair Information Practice) 对美国联邦机构记录系统中保存的有关个人身份信息的收集、存储、使用和传播进行规范。
网络安全法	中国	2017	保障网络安全，维护网络空间主权、国家安全和公共利益，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。

法律法规	国家或组织	发布日期	概要
个人信息保护法 (Act on the Protection of Personal Information)	日本	2003	2003 年 5 月 23 日颁布的《个人信息保护法》(2003 年第 57 号法) 对私营部门进行规范。
保障个人资料条例草案 Protection of Personal Information Bill	南非	2009	该法案旨在促进个人隐私权，并使南非符合相关国际数据保护法。
Data Protection Act 数据保护法	英国	2018	《1998 年数据保护法》是英国议会的一项法案，旨在保护存储在计算机或有组织的文件归档系统中的个人数据。它颁布了《1995 年欧盟数据保护指令》中关于数据保护、处理和移动的规定。该法案被《2018 年英国数据保护法》取代。
Personal Information Protection and Electronic Documents Act 个人信息保护与电子文件法	加拿大	2019	其规定个人信息包括关于记录的或未记录的可识别个人的任何事实或主观信息，包括任何形式的信息。

第二章 在线学习中的个人数据和隐私

2.1 个人数据

个人信息

个人信息是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特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

—中华人民共和国民法典，第一千零三十四条

个人数据，亦称为个人信息或个人识别信息 (personally identifiable information，PII)，是指与可识别人有关的任何资料。在以《通用数据保护条例》（General Data Protection Regulation，GDPR）为核心的欧洲和其他国家和地区，“个人数据”（Personal data）一词被广泛使用。各国家和国际组织关于个人信息的定义见表 2-1。

表 2-1：部分国家和国际组织有关个人信息的定义

法律法规	国家或组织	个人信息的定义
ISO/IEC 29100:2011 国际标准	国际标准化组织 (International Organization for Standardization，ISO)	任何信息，可用于识别与这些信息相关的主体或者是或可能直接或间接与主体相关。

法律法规	国家或组织	个人信息的定义
保护隐私及个人数据跨境流动指引 (Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)	经济合作与发展组织（Organization for Economic Co-operation and Development, OECD）	个人数据指任何与已识别或可识别的个人 (数据主体) 有关的资料。
个人数据 : 一种新的资产分类的出现（Personal Data: The Emergence of a New Asset Class）	世界经济论坛（The World Economic Forum）	个人数据定义为由人们创建和关于人们的数据 (和元数据)，包括： 个人自愿创建和明确共享的数据，例如社交网络文档。 观测数据——记录个人行动的数据，例如使用手机时的位置数据。 推断数据——基于自愿或观察信息分析的个人数据，例如信用评分。
通用数据保护条例 (General Data Protection Regulation, GDPR)	欧盟	个人数据指任何与已识别或可识别的自然人 (数据当事人) 有关的资料。
个人身份信息保密性保护指南（NIST SP 800-122 Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)）	美国	由机构保存的关于个人的任何信息，包括可用于识别或追踪个人身份的任何信息，如姓名、社会保障号码、出生日期和地点、母亲的婚前姓名或生物识别记录 ; 以及与个人有关联或可关联的任何其他信息，如医疗、教育、财务和就业信息。
网络安全法	中国	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。

(1) 个人信息的类别

个人信息是一个复杂的概念，它包括许多种类。了解个人信息的分类，有助提升个人信息保护的意识，并更好地掌握个人信息保护的方法。许多国家和国际组织都对个人数据进行了分类，这些分类是非常相似的。

根据电气电子工程师协会（Institute of Electrical and Electronics Engineers，IEEE）的出版物《伦理一致的设计：人工智能和自主系统优先考虑人类福祉的愿景》（Ethically Aligned Design: A Vision for Prioritizing Human Wellbeing with Artificial Intelligence and Autonomous Systems），数字人物（digital persona）是为了代表可能使用网站或产品的不同用户创建的虚拟用户，如图 2-1 所示。它包括健康数据、政府数据、教育数据、交通数据、移民数据、消费者和忠诚度数据、电信数据、媒体和内容数据、税收和就业数据、在线论坛、投票和党派关系数据、保险和法律数据、银行和金融数据和数字继承数据等。

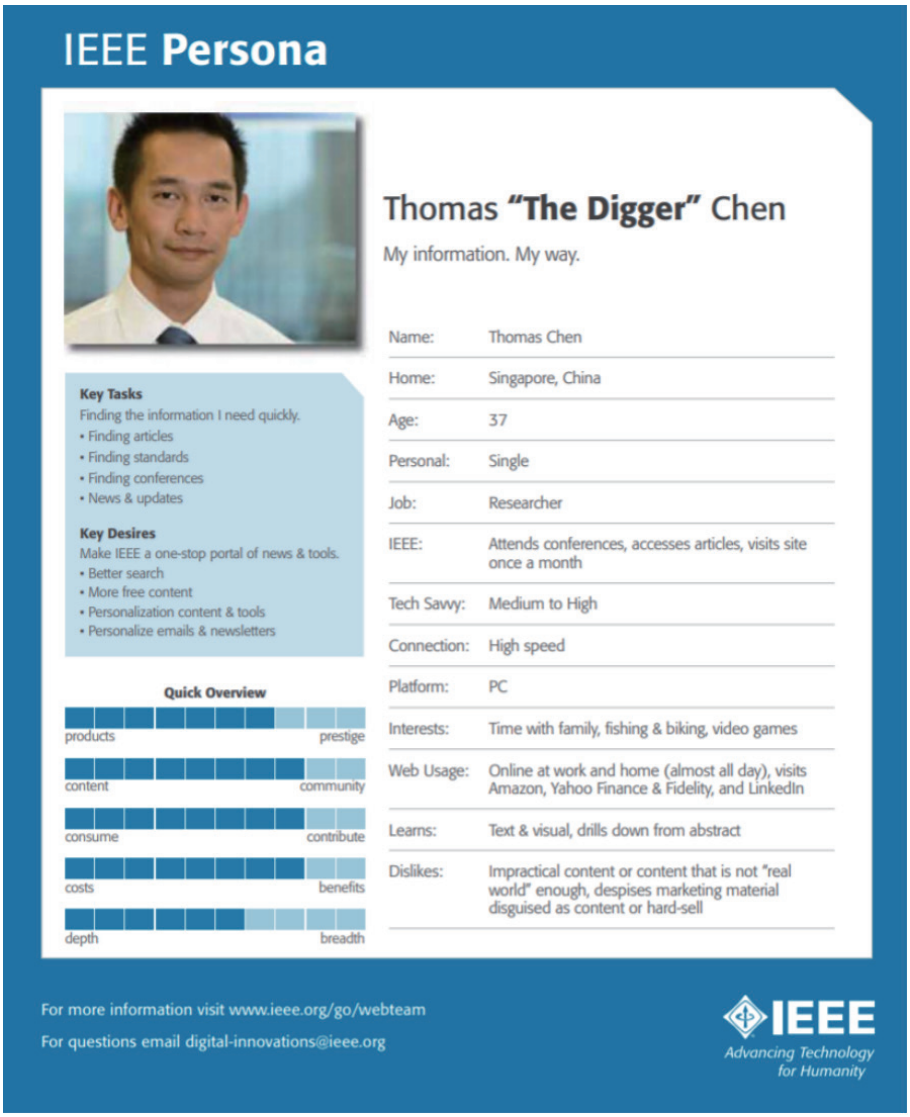


图 2-1:IEEE 的数字人物举例

隐私权专家国际协会 (International Association of Privacy Professionals, IAPP) 将个人信息分为六大类：内部、外部、历史、金融、社会和跟踪，具体包含 24 种类型。

中国国家标准《信息安全技术—个人信息安全规范》（GB/T 35273-2017）中，个人数据被分为两个级别 (个人信息、个人敏感信息) 和 13 个更详细的类别。美国加州消费者隐私法 (California Consumer Privacy Act，CCPA) 的分类更偏向于与消费和购买行为相关的个人信息。

在所有分类中，我们都可以看到个人身份数据、财务数据、健康数据等类别。但在某些分类中，没有涵盖与个人社交生活和个人跟踪信息相关的内容。结合各种分类的不同特点和共性，我们对个人数据的分类方法进行总结，如表 2-2 所示。

表 2-2：个人信息分类

基本信息	姓名，年龄，出生地，出生日期，性别，性别认同，偏好，倾向，个人照片，种族，肤色，民族或族裔
身份识别信息	身份证，驾驶证，护照，健康证，社会保险号码
生物信息	基因，指纹，声纹，掌纹，耳廓，虹膜，面部特征
认证信息	密码，个人密码，系统帐户，IP 地址，电子邮件地址 , 安全答案，个人数字证书
医疗及健康信息	身体和心理健康，家庭或个人健康史，健康记录，病史，药物测试结果，残疾信息，血型，DNA
职业信息	职位名称，工资，工作经历，就读学校，教育经历，员工档案，就业经历，评估，推荐信，面试，雇主数据，证书，纪律处分
财务信息	汽车，房子，公寓，个人财产，购买，销售，信用，收入，贷款记录，交易，税收，购买和消费习惯，信用记录，信用评分，信用状况，信用能力，实物资产和虚拟物品
通信信息	电话号码，通话记录，通话录音，短信，电子邮件，即时通信平台账号
联络信息	通讯录，朋友，联系人，熟人，协会，团体

浏览历史	文本、音频、照片、视频和其他形式的媒体；真实世界和在线情景、活动、兴趣和行为：位置、时间、点击、搜索、浏览器历史记录和日历数据、购买活动、网上购物、社交网络档案信息等
设备信息	序列号（IMEI），IP 地址，MAC 地址
位置信息	国家，城市，经纬度，常去地点，特定时间的行动路线等

(2) 个人数据的生命周期

数据生命周期是特定数据单元从最初的生成或采集，到生命周期结束时最终归档或删除所经历的一系列阶段。根据联合国教科文组织教育信息技术研究所发布的《在线教育平台个人数据安全技术指南》，数据生命周期包括采集、传输、使用、存储和销毁五个阶段。

1) 采集

在线平台采集数据应符合安全基本原则，应在数据产生时按照数据类型、敏感程度、数据价值等属性明确数据分类、分级标准，并统一对数据进行分类分级标志；在收集使用未成年人信息时应当取得监护人同意或授权。当数据被标记为个人信息或与个人信息主体有关的附加信息时，应实施隐私控制。

2) 传输

为了确保数据传输安全，在线平台应该在数据传输过程中建立适当的保护机制，使用网络安全协议，如 TLS，IPsec 等，并使用相关标准推荐的加密算法。

3) 使用

平台应提供统一的权限管理，确保用户按照最小权限原则随需应用和访问相关数据。在线平台应为使用和访问相关数据提供全面的安全监测和访问审计措施，以及个人信息保护机制（包括但不限于隐私保护技术，如去身份和伪匿名化技术）。

4) 存储

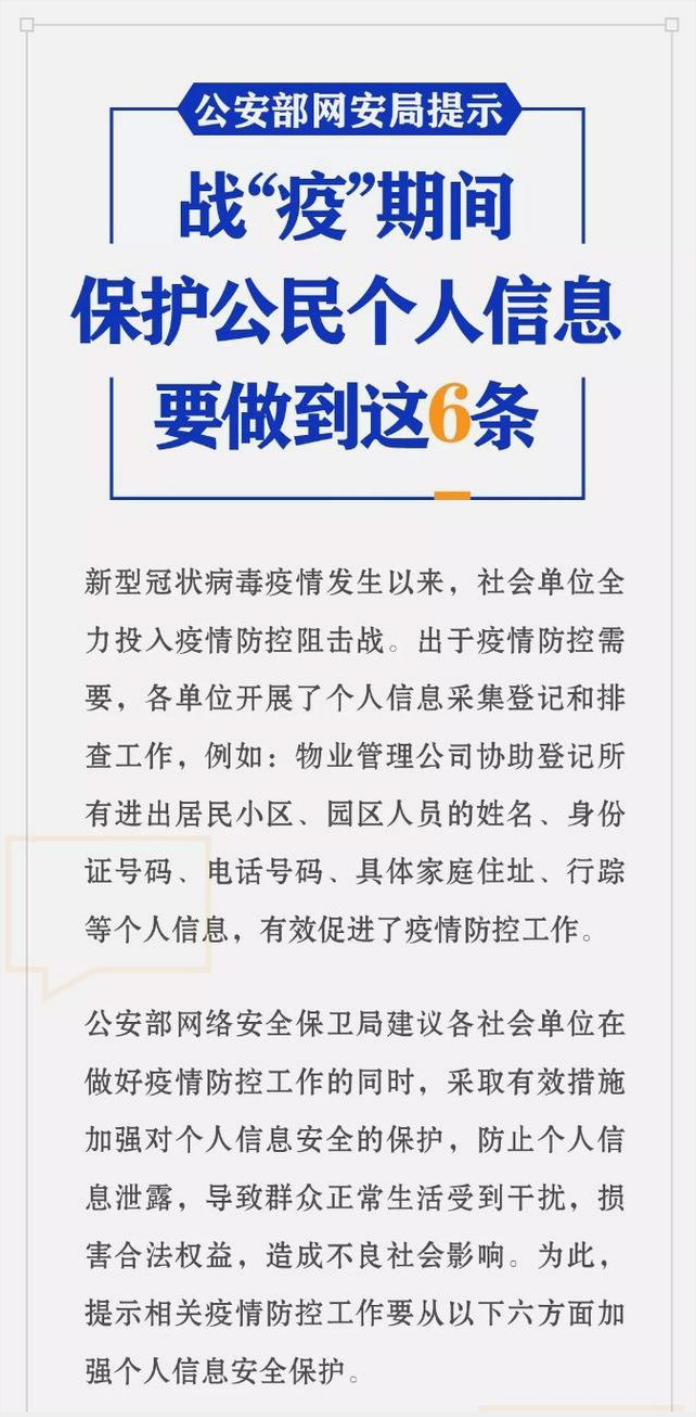
在线平台的数据存储应遵循安全原则，通过访问控制和安全保护，防止未经授权的访问、修改、销毁、删除或其他使用。这些机制包括但不限于加密、签名、匿名化、密钥管理等。在线平台应具备高可用性、数据备份和灾难恢复能力，确保数据的可靠性和可用性。

5) 销毁

在线平台应根据数据分类和存储介质对数据进行销毁。在删除信息处理设施和存储介质之前，应按照相关标准进行数据删除和物理销毁，避免数据泄露的风险。

扩展阅读

战“疫”期间保护公民个人信息要做到这 6 条



1

采集个人信息应遵循目的限定原则，合理确定个人信息采集范围，避免采集与疫情防控无关的个人信息。

2

使用个人信息应严格限定使用范围，为疫情排查收集的个人信息，不用于其他用途。

3

对信息系统采集的个人信息，应采取访问控制、加密存储和审计等必要措施，确保采集的个人信息，特别是个人敏感信息不被泄露、篡改、毁损。

4

以纸质填表方式登记个人信息的，应严格管理纸质材料，妥善保管、使用、销毁。

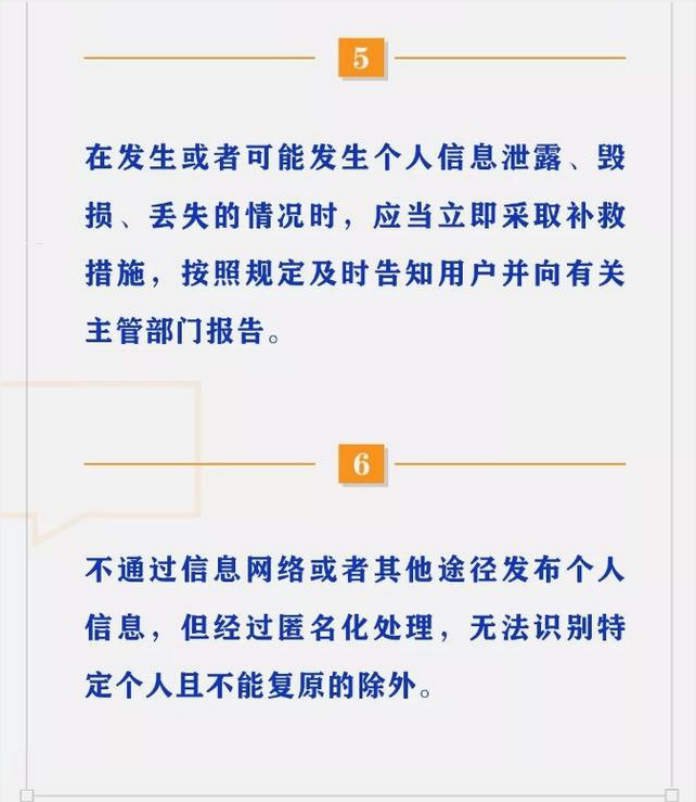


图 2-2：战“疫”期间保护公民个人信息

2.2 学生数据和隐私

在教育领域，学生数据是指教育者、学校和在线服务商收集的学生个人信息，相当于学生的教育记录。高质量的教育数据可以帮助提升学生在学校的表现，并帮助他们为成功的人生做好准备。如果这些数据得到有效利用，就可以使教育者、学生和家庭获得他们做出决定所需的信息，从而帮助所有的学生取得成功。

教育记录

“教育记录”是与学生直接有关的记录，由教育机构或代表该机构的当事方保存。这些记录包括但不限于年级、成绩单、班级名单、学生课程时间表、健康记录 (K-12 年级)、学生财务资料 （高等教育阶段）和学生纪律档案。信息可以以任何方式记录，包括但不限于手写、印刷、计算机媒体、录像带、录音磁带、胶片、缩微胶片和电子邮件。

- 34 CFR § 99.2，美国家庭教育权利和隐私权法案（Family Educational Rights and Privacy Act of United States）

(1) 学生数据由什么组成?

传统的学生数据包括出勤率、成绩、纪律记录和健康记录等。过去，只有行政人员、指导顾问、教师或其他学校官员才能获取这些数据，因为他们需要这些数据来满足学生的教育需求。

随着技术在学校中的应用，传统的学生数据现在经常与提供学生信息系统（Student Information Systems，SIS）、学习管理系统（Learning Management Systems，LMS）和许多技术的公司共享。家长、学生已经提出了关于哪些信息正在被收集或共享，以及这些公司将如何使用这些数据的问题。

学生个人信息包括有关学生身份、学术背景、医疗状况的任何信息，或者由学校或技术供应商代表学校收集、储存和传播的任何其他信息。这包括：

- 姓名
- 联系方式，出生日期，身份证明文件
- 父母，兄弟姐妹和家庭的详细资料
- 被收养的孩子，在特殊监护下照看的孩子的信息
- 各种测试的结果记录
- 课程学习纪录
- 特征，如种族背景，语言，奖学金或特殊教育需要
- 退学、肄业或开除学籍的信息
- 任何健康状况的记录，包括身体和精神健康
- 出勤资料
- 安保信息
- 获得的任何援助信息，包括各种福利计划，爱心人士信息
- 儿童照片
- 教育应用程序
- 视频监控

(2) 学生数据的价值

数据是最强大的工具之一，可以在学生的教育历程中为他们提供信息、参与活动并创造机会，这些数据不止是考试成绩。数据帮助我们更好地洞察和改进行为。如图 2-3 所示，对学生来说，学生数据有助于更好地了解自己的学习风格和能力，塑造自己的成长过程。对家长来说，学生数据帮助了解应该采取什么行动来帮助孩子走上成功的道路。对老师来说，学生数据可以帮助了解学生在哪些方面取得了成功，在哪些方面遇到了困难，从而提供相应的帮助。对学校管理者来说，学生数据可以帮助了解什么在学校起作用，什么在学校不起作用，从而及时做出决定，确保资源更好地支持教学、改善学生的学习。对课外辅导员来说，学生数据可以帮助了解学生在上学前发生了什么，从而帮助家庭和社区为学生创造更多的成功机会。

图 2-3：学生数据对利益相关者的价值

数据可以将教育转化为个性化的体验，满足个人的需求，并确保没有学生在学习过程中掉队。从家长到政策制定者，教育利益相关者以不同的方式使用不同类型的数据（包括考试成绩、课程成绩和人口统计信息）来改善学生的教育。

扩展阅读

使用和保护学生个人信息的基本原则

1. 学生数据应该用来支持学生的学习，帮助学生获得成功。
2. 学生数据对于持续进步和个性化学习十分重要。
3. 学生数据应该被当作一种工具，让学生、家庭、教师和教育管理者了解情况并给学生赋能。
4. 学生、家庭和教育工作者应及时获得有关学生的信息。
5. 学生数据应该作为辅助信息，而不是取代教育者的专业判断。
6. 学生的个人信息只能出于合法的教育目的，根据协议或条款与服务提供商共享，否则，共享必须得到家长、监护人或超过 18 岁的学生的同意。教育系统应该有监督这一过程的政策，包括对教师的指导。
7. 教育机构和他们的外包服务提供商，以及研究人员，应该有明确的、公开的规范来指导他们如何收集、使用、保护和销毁学生数据。
8. 教育工作者及其外包服务提供商只能获得最低限度的学生数据。
9. 每个能够接触到学生个人信息的人都应该接受培训，并且知道如何有效和合乎道德地使用、保护这些信息。

(摘自 https://studentdataprinciples.org/the-principles/)

（1）学生数据隐私

隐私

隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。

— 中华人民共和国民法典，第一千零三十二条

广义而言，隐私权是指不受干扰或侵犯的权利。信息隐私权是指对个人信息的收集和使用有一定控制权的权利。

根据经济合作与发展组织 (OECD) 的《保护隐私和个人数据跨界流动准则》（Guidelines on the Protection of Privacy and Transborder Flows of Personal Data），有一种倾向是扩大传统的隐私概念（不受干扰的权利），并确定一种更为复杂的利益综合体，或许更准确地称之为隐私和个人自由。

具体而言，隐私可以分为四类：1) 身体方面：限制他人通过一种或多种人类感官体验一个人或一种情况；2) 信息方面：限制搜索或揭露他人不知道或不知道的事实；3) 决策方面：限制干涉某一实体独有的决定；4) 性格方面：限制试图了解一个人的精神状态。

学生数据隐私涵盖学生个人身份信息（PII）的使用、收集、处理和管理。这包括任何所有可以用来识别、定位或联系个别学生的信息。

对于学校管理者来说，学生数据隐私这个话题从未像现在这样受到关注。尽管这个话题从 20 世纪 70 年代学校开始收集电子信息时就已经存在了，但是随着互联网与教育的不断融合，很多事情都发生了改变。数字世界的规模爆炸式增长，大多数学校都依赖于云服务来收集和存储数据，其涉及学生数据隐私，管理人员面临着前所未有的风险和责任。

在收集、使用、共享和处理学生个人信息方面存在法律和道德限制。与此同时，学校内外的数据收集和学生信息的使用也在不断增加。此外，管理人员正在将数据服务外包，并将更多的技术引入课堂，与信息技术服务和解决方案提供商签订的合同数量增加，学校管理的合同也越来越多。这种变化应该为所有管理人员敲响警钟。底线是学校在法律和道德上有义务保护学生个人数据——不管学生数据在哪里、如何创建、使用或存储。

2.3 隐私保护框架

隐私政策

隐私政策是一种声明或法律文件（隐私法），它公开了一方收集、使用、披露和管理客户或客户数据的部分或全部方式。 个人信息可以是任何可以用来识别个人的东西，不仅限于个人的姓名、地址、出生日期、婚姻状况、联系信息、身份证签发和到期日期、财务记录、信用信息、病史、旅行地点以及购买商品和服务的意图。

– McCormick, Michelle. “New Privacy Legislation.” Beyond Numbers 427 (2003): 10-. ProQuest. Web. 27 Oct. 2011

随着创新技术的发展步入新时代，越来越多的数据被收集和交换，隐私正变得越来越复杂。数据的使用也随着技术革新而变得越来越复杂。这使得在线学习工具提供商这样的组织为确保个人信息得到保护而面临难以置信的复杂局面。

各组织被要求落实“适当的技术和组织措施”，以确保他们按照隐私法律和条例规定来处理个人数据，他们还必须遵守问责制原则。这意味着他们要对法律约定的数据处理原则负责，并且能够证明他们遵守了这些原则。

这可以通过一个管理个人数据安全的框架——隐私保护框架来实现。这些框架和原则由目的、范围和原则三部分组成。

《联合国个人数据和隐私保护原则》（Personal Data Protection and Privacy Principles）是由三十个联合国机构组成的隐私政策小组（PPG）在两年的时间里起草的。自 2016 年年底启动联合国“全球脉动”倡议以来，教科文组织根据其促进互联网普遍性 ROAM 框架 (人权、开放、获得、多方利益相关者) 的全球任务，加入了隐私政策小组并为其作出了贡献。

这些原则的目的包括：

- 统一联合国体系内保护个人数据的标准
- 为执行联合国体系各组织的任务，促进对个人数据进行问责处理
- 确保尊重个人的人权和基本自由，特别是隐私权

各成员国认识到保护隐私权在利用数据和技术促进《2030 年可持续发展议程》起到作用，这些隐私权原则具有重要意义。

教科文组织在教育和能力建设方面负有特殊使命，坚定地在全球和组织内推行这些原则。隐私和个人数据保护是联合国教科文组织推动的数字技能的一部分。教科文组织已同意将这些原则纳入它的政策，并正在制定进一步的指导方针，以便在执行任务和日常工作时保护个人数据和隐私。

除联合国个人数据和隐私保护原则外，经济合作与发展组织 (OECD) 隐私框架、亚太经合组织 (APEC) 隐私框架、国际标准化组织 ISO 和国际电工委员会 IEC 的 ISO/IEC27701-2019 隐私信息管理体系 (PIMS) 等也是国际公认的隐私保护原则框架和标准。隐私政策应涵盖以下几点：

- 清晰易懂的陈述（透明原则）
- 网站或应用程序所收集的资料类别 (有限的收集及使用)
- 数据存储和使用（数据生命周期管理)
- 如何保护数据（设计安全性)
- 用户如何管理其数据（数据当事人权利)

扩展阅读

授权管理平台 (CMP)

授权管理是一个过程，它要求网站在授权收集时满足法律或监管要求。有了授权管理平台 (CMP)，网站就有了技术能力，可以告知访问者他们将收集的数据类型，并就特定的数据处理目的征求他们的同意。CMP 提供了一套隐私保障程序，使收集或处理个人信息的组织能够证明负责任的数据收集和处理实践与监管期望和隐私问责的外部标准一致。以下是五个常见的授权管理平台。

Piwik PRO 强调坚持大西洋两岸最严格的隐私标准，无论是 GDPR 还是 HIPAA。Piwik PRO 成立于 2013 年，是一家定制 AdTech 软件公司 Clearcode 的投资组合公司。它为从银行到公共部门组织的数据敏感客户提供服务。

TrustArc (前身为 TRUSTe) 是一个总部位于旧金山的数据隐私管理平台，其在美洲、欧洲和亚洲均设有办事处。TrustArc 平台提供专家咨询和经过验证的方法，帮助组织处理隐私项目管理的所有阶段。它也是第一个在 2000 年加入安全港框架的组织。

OneTrust 成立于 2016 年，支持各组织展示问责性并遵守多项全球法规。这家年轻的公司在亚特兰大、乔治亚州和英国伦敦设有办事处，是一个正迅速获得认可的快速发展和可靠的隐私管理技术平台。

Cookiebot 是一个由 Cybot 创建的 cookie 和在线跟踪授权解决方案。该公司总部设在丹麦的哥本哈根。它提供自动化的电子隐私服务，要求网站运营商尊重和保护访问者的隐私。

Consentmanager.net 是一个授权管理提供商，项目的总部设在瑞典的韦斯特罗斯。 Consentmanager.net 已经被广泛用来协助报纸、广告公司和网络服务商。

2.4 在线学习数据收集

随着个人电脑、移动设备、应用程序和在线学习工具在课堂上的应用，产生了海量的学生数据，无论是昨晚的数学作业，还是学生在应用程序中的行为表现的元数据，亦或学生、老师和家长的相互交流，大部分都是由第三方服务提供商收集、保存和处理的。

(1) 什么是元数据?

元数据（metadata）是帮助描述其他数据的数据。如今，元数据是电子化的，但从历史上看，它曾包含在图书馆的卡片目录中。元数据由电脑程序和人工共同生成的标签组成。

在大多数网站上，元数据的形式是各种的标签，以帮助其他网站和应用程序理解它具体是关于哪些方面。例如，如果不使用元数据，一个教育网站描述大学的地址时可能会说：“这所大学在北京，在新街口外大街。”为了让机器和人们更容易检索和了解这所大学，网站可能会将这些关于地址的数据转换成元数据：“北京”和“新街口外大街”。

(2) 教育元数据

元数据的含义超越了隐私。在教育领域，技术为学生提供了“个性化”学习体验的潜力，元数据至关重要。资源上的元数据越全面，其他工具和服务就越容易使用。元数据为通过个性化学习平台获取在线学习资源提供了巨大的潜力。

随着各种在线学习工具与学生、老师、家长的联系日益紧密，隐私成为重中之重。除了之前介绍的学生数据，我们还应该注意 “教育元数据”。

根据教育部研究制定的《基础教育教学资源元数据》系列中国教育行业标准，包括《基础教育教学资源元数据 信息模型》《基础教育教学资源元数据 XML 绑定》《基础教育教学资源元数据 实践指南》等，关于教育的元数据是指对基础教育教学资源的描述信息。

教育元数据在在线教育领域，为各类数据提供含义和解释，例如，如果知道学生完成一项在线任务的日期和时间、学生尝试了多少次以及学生的鼠标在一个项目上停留了多长时间 (可能表示犹豫不决)，那么关于某个特定学生完成一项在线任务花费了多长时间的信息就更有意义。对教育元数据的规范和充分使用，是完善教育信息化标准体系，保障教育信息化健康有序发展的重要手段。

扩展阅读

共享内容对象参考模型 SCORM

共享内容对象参考模型 (SCORM) 是基于网络的电子教育技术 (也称为 E-learning) 的标准和规范的集合。它定义了客户端内容和主机系统 (称为“运行时环境”) 之间的通信，通常由学习管理系统支持。SCORM 还定义了如何将内容打包成可转移的 ZIP 文件，称为“包交换格式”。

SCORM2004 引入了一个叫做序列的复杂思想，这是一套规定了学习者体验内容对象的顺序的规则。简单

来说，这些规则通过训练教材将学习者限制在一套固定的路径上，允许学习者在休息时将自己的学习进度“标记”，并确保学习者在考试中取得的成绩是可接受的。该标准使用 XML，基于 AICC、IMSGlobal、IEEE 和 Ariadne 的工作成果。

2.5 个人对数据的权力

在线服务收集越来越多的用户个人数据，并利用这些数据提取有价值的用户信息。这些数据可以用于提供新的服务和个人特征分析，其结果是可以盈利的投放，例如有针对性的广告。然而，个人通常很少或根本无法控制他们的数据是如何创建或使用的。

作为一个数字公民和在线学习者，了解这些权利以确保你在使用互联网时的安全是很重要的。

隐私法赋予人们保留个人信息的权利。根据各国的隐私保护法，以下是个人对其个人信息拥有的权利：

- 数据访问权
- 被遗忘权
- 数据可移植和可携带权
- 知情权
- 修改权
- 限制数据处理权
- 反对权

扩展阅读

中国国家互联网信息办公室，工业和信息化部等四部门制定的《App 违法违规收集使用个人信息行为认定方法》

以下行为可被认定为“未公开收集使用规则”

1. 在 App 中没有隐私政策，或者隐私政策中没有收集使用个人信息规则；

2. 在 App 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；

3. 隐私政策等收集使用规则难以访问，如进入 App 主界面后，需多于 4 次点击等操作才能访问到；

4. 隐私政策等收集使用规则难以阅读，如文字过小过密、颜色过淡、模糊不清，或未提供简体中文版等。

以下行为可被认定为“未明示收集使用个人信息的目的、方式和范围”

1. 未逐一列出 App(包括委托的第三方或嵌入的第三方代码、插件) 收集使用个人信息的目的、方式、范围等；

2. 收集使用个人信息的目的、方式、范围发生变化时，未以适当方式通知用户，适当方式包括更新隐私政策等收集使用规则并提醒用户阅读等；

3. 在申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解；

4. 有关收集使用规则的内容晦涩难懂、冗长繁琐，用户难以理解，如使用大量专业术语等。

以下行为可被认定为“未经用户同意收集使用个人信息”

1. 征得用户同意前就开始收集个人信息或打开可收集个人信息的权限；

2. 用户明确表示不同意后，仍收集个人信息或打开可收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用；

3. 实际收集的个人信息或打开的可收集个人信息权限超出用户授权范围；

4. 以默认选择同意隐私政策等非明示方式征求用户同意；

5. 未经用户同意更改其设置的可收集个人信息权限状态，如 App 更新时自动将用户设置的权限恢复到默认状态；

6. 利用用户个人信息和算法定向推送信息，未提供非定向推送信息的选项；

7. 以欺诈、诱骗等不正当方式误导用户同意收集个人信息或打开可收集个人信息的权限，如故意欺瞒、掩饰收集使用个人信息的真实目的；

8. 未向用户提供撤回同意收集个人信息的途径、方式；

9. 违反其所声明的收集使用规则，收集使用个人信息。

第三章 个人设备设置和学习工具选择

开始在线学习之前，应该准备好设备、网络，下载学习工具，阅读隐私政策等。这些不仅可以帮助保护个人数据，同时也可以保证在线学习的质量。

3.1 设置个人设备

级别	认识 / 警惕 / 保护自己 / 保护他人
相关用户	学生、家长、老师
相关隐私	储存在设备内的个人数据，例如个人身份信息
风险	遗失或被盗

要保护个人数据，首先要确保电子设备的设置正确，这包括设备的选择以及设备的安全性。

主题：我可以选择哪些设备？

1) 平板电脑和智能手机

它们轻便、可移动、可触控，并且操作起来相对简单，适合所有年龄段的人使用。写作、绘画、拍摄照片、录像以及录音等功能使用起来都十分便利。

2) 笔记本电脑

它们拥有平板电脑所没有的集成键盘。因为便携，所以它们可以在不同的环境中使用。

3) 台式电脑

台式电脑可能拥有更完整的键盘和更大的屏幕，通过使用有线的方式连接网络，在进行学习时会有更好的网络稳定性。

主题：如何确保设备安全？

- 注意设备上的摄像头和麦克风
- 在公众场所注意保管好个人设备，以防盗窃
- 锁定你的设备，设置安全的密码
- 及时更新，确保设备使用最新的操作系统
- 安装杀毒软件
- 不要“越狱”，不要获取手机的根权限
- 定期备份重要的个人资料

3.2 管理网络连接

级别	认识 / 警惕 / 保护自己 / 保护他人
相关用户	学生、家长、老师
相关隐私	储存在设备内的个人数据，例如个人身份信息
风险	· 网络入侵 · 中间人攻击 · 浏览器劫持

安全的网络可以防止未经授权的用户和黑客访问你的网络。安全地连接和使用网络十分重要。

WiFi

WiFi 是一种将电子设备连接到无线局域网 (WLAN) 的技术。 WiFi 通常被称为无线网络。

主题：如何将移动设备连接到互联网？

1) 4G 连接

手机设备通过网络运营商的提供的蜂窝网络联网。通过 4G 发送的数据是加密的，一般来说，4G 比公共 WiFi 更安全。

2) 私人 WiFi 连接

私人 WiFi 连接如果设置得当，就可以对发送和接收的数据进行加密保护。

3) 公共 WiFi 连接

公共 WiFi 通常出现在机场、咖啡店、酒店等公共场所。公共 WiFi 是连接互联网最不安全的方式。

虚拟专用网络 (VPN)

虚拟专用网络 (VPN) 将专用网络扩展至公共网络，使用户能够通过共享网络或公共网络发送和接收数据，就好像他们的计算设备直接连接到专用网络一样。VPN 是通过使用专用电路或使用现有网络上的隧道协议建立虚拟的点对点连接而创建的。

主题：如何安全使用互联网？

通过 WiFi 连接比通过 4G 连接更容易被攻击者利用安全漏洞破解和窃取信息。以下各种连接从最安全到最不安全的排序：

- 通过虚拟专用网络通道使用蜂窝网络或 WiFi
- 蜂窝网络
- WiFi

3.3 选择和安装学习工具

级别	认识 / 警惕 / 保护自己 / 保护他人
相关用户	学生、家长、老师
相关隐私	个人身份信息，生物识别信息
风险	· 假冒或恶意网站 · 电脑病毒 · 恶意软件

在选择、下载和安装在线学习工具时，我们应该注意什么？这里有一些建议。

主题：作为一名教师，我如何为学生选择工具？

在选择在线学习工具时，要考虑以下几点：

1) 适合性

考虑这些工具是否符合你的教学目的，工具是否会对你的教学起到负面作用。

2) 易用性

在决定是否选择某个工具时，作为新用户来评估该工具。尝试确定你的学生入门和熟练使用此工具的困难程度，以便他们能够有效地使用工具来参与学习。

3) 无障碍性

确保选择无障碍性的工具，如通用学习设计原则 (Universal Design for Learning，UDL) 所定义的灵活、适应性强的课程设计，支持多种学习方法，促进所有学生积极参与，满足特定的残疾学习者可访问性需求的强制性标准等。

4) 必需的设备

在选择工具时，你可能需要调查学生对技术的掌握情况。例如，学生可能无法使用网络摄像头或麦克风，这将影响他们进行在线学习。

安全套接层字层协议 (SSL)

SSL 是在 TCP/IP 协议之上实现的安全协议。SSL 支持各种网络，并提供三种基本安全服务，所有这些服务都是由一个公钥和一个对称密钥启用的。

主题：如何安全下载及安装软件？

1）注意网站地址。通过使用主流的浏览器（Google Chrome，Edge，Firefox，Safari），会对不安全的网址进行风险提示。

2）注意分辨网址是否为官方网址。如下图，第一个为苹果的官方网址（apple.com），第二个为非官方的网址（s***apple***.com）。

3）从正规来源下载：从官方网站和操作系统自己的应用商店安装软件，如微软商店、苹果应用商店、华为应用市场等。

4）注意扣费信息：是否免费试用后会自动开始扣费，是否存在自动续费等。

3.4 浏览隐私政策

级别	认识 / 提高警觉
相关用户	学生、家长、老师
相关隐私	基本资料
风险	在线学习工具滥用数据

全球有很多隐私法都要求企业向其客户提供隐私政策。它通常会详细说明有关你数据的重要法律信息，包括收集什么信息、如何使用这些信息、与谁共享这些信息，以及如何保护这些信息。学习者在下载和安装各类学习工具时应该仔细阅读这些隐私政策。

主题：如何找到隐私政策?

1)  **微信**

隐私政策网址 : https://www.wechat.com/zh_CN/privacy_policy.html

在安卓上找到：我—设置—关于微信—隐私保护指引

在 iOS 上找到：我—设置—关于微信—隐私保护指引

2)  **QQ**

隐私政策网：https://ti.qq.com/agreement/qqface.html?appname=mqq_2019

在安卓上找到：你的头像—设置—关于 QQ 与帮助—隐私保护指引

在 iOS 上找到：你的头像—设置—关于 QQ 与帮助—隐私保护指引

3)  **Zoom**

隐私政策网址：https://zoom.us/Privacy

在安卓上找到：设置—隐私政策

在 iOS 上找到：设置—隐私政策

4) IXL

隐私政策网址：https://www.ixl.com/privacypolicy

在安卓上找到：你的个人资料—头像头像—关于我们—隐私政策

在 iOS 上找到：你的个人资料头像—设置—关于 IXL 隐私政策

5) Edmodo

隐私政策网址：https://go.edmodo.com/Privacy-Policy

在 Android 上查找：创建免费帐户—选择你是谁—隐私政策

在 iOS 上查找：创建免费帐户—选择你是谁—隐私政策

扩展阅读

1) 正确选择数字设备

本指南将为你提供可以帮助你决定选择进行在线学习的设备的信息。选择设备时，不仅要考虑这些设备本身如何，还要考虑它们的使用方法、哪种设备最适合哪种类型的活动，以便有效地教学和学习。该指南也有助于学校向家长提供购买哪种设备的建议。

链接 : http://elearning.tki.org.nz/Technologies/Technical-support-and-procurement/CLA-resources/Choosing-the-right-digital-device

2) 教育技术和数字学习

有关教育技术的数据和研究分为两个部分。第一部分集中讨论教室中各种技术设备的提供或使用以及诸如互联网接入等其他主题。第二部分着重于在线学习，提供有关其流行程度的数据和学生可获得的不同类型的在线学习。每个部分最后都回顾了所讨论的技术的有效性以及对学生学习成果的影响。

链接：https://nsf.gov/statistics/2018/nsb20181/report/sections/elementary-and-secondary-mathematics-and-science-education/instructional-technology-and-digital-learninginstructional-technology-and-digital-learning

3) 在学校关闭期间，如何为你的学生找到好的学习资源?

不管你是否习惯用技术来教学，逐渐将教学方式向远程学习过渡仍是一项艰巨的任务。学生的年龄、使用技术的途径、为学习列出的目标和期望，这些因素都影响着你如何选择工具和平台。我们在这里提供借鉴与支持，以方便你选择最适合你和你的学生的工具。这里有关于每个应用程序、网站的优点、缺点和“操作指南”以及成千上万的评论。为了更容易地筛选这些评论，我们将这些评论收集到了精选名单。

链接：https://www.commonsense.org/education/articles/how-to-find-great-learning-resources-for-your-students-during-school-closures

4) 远程学习和虚拟教室平台

以下链接中提供的网站允许教师通过创建自己的在线学习资源来开展现有的教学计划。有些还提供了托管虚拟交互式多媒体教室的平台。

链接：https://www.com/free-online-learning-resources/#plat-forms

5) 学生隐私承诺书

“未来隐私论坛”（Future of Privacy Forum）和美国软件和信息产业协会（Software and Information Industry Association）推出了《学生隐私承诺书》，在收集、维护和使用学生个人信息方面，保护学生的隐私。你可以在下面找到所有签署应用隐私政策的链接。

链接： https://studentprivacypledge.org/signatories/

第四章 注册和登录时的隐私安全

用户在登录学习平台时，往往需要先进行注册。用户在这个过程中可能会发生个人信息的泄露。

4.1 创建账户的密码策略

级别	认识 / 提高警觉 / 保护自己
相关用户	学生、家长、老师
相关隐私	个人身份信息，网络身份信息
风险	· 弱密码 · 密码泄露

注册用户通常向系统提供某种凭证（如用户名或电子邮件地址和密码）以证明其身份。设置强密码、防止密码泄露、防止生物特征信息被滥用对用户来说至关重要。

主题：如何设置强密码？

- 至少包含 8 个及以上字符
- 最好包含四种不同类型的字符：大写 / 小写字母、数字和特殊字符，如 */” &
- 不应该是任何语言中的一个名字或单词
- 不应该包括你的姓名，地址或出生日期的任何部分
- 不同服务或网站应使用不同的密码

主题：使用密码管理工具

密码管理工具是管理密码的良好方式。它们可以安全存储你的密码，一些还提供了备份密码和多系统同步密码的方法。可以在苹果 App Store，各大主流安卓应用市场搜索相关应用。

主题：如何使用谷歌浏览器或 iOS 生成强密码?

当你创建在线帐户时，有一些规则，如“密码必须至少 8 个字符”，“密码必须至少包含一个大写字母”等等。你可以让 Google Chrome 浏览器或 iPhone 为你的许多账户设置强密码，也可以自己设置密码。

使用谷歌浏览器生成密码

获得最新的官方操作指南，请访问

https://support.google.com/chrome/answer/7570435?co=GENIE.Platform%3DiOS&hl=en&oco=0

1) 在安卓系统上

a) 打开 Chrome 的同步功能。
b) 登录一个网站，注册一个账号。
c) 点击密码文本框。
d) 点击建议强密码。
e) 如果你没有看到这个选项，点击 -- 密码 -- 建议强密码。
f) 你可以看到密码的预览。要确认，请点击“使用密码”。
g) 完成注册后，你的密码会自动保存到 Chrome 中。

2) 在 PC 端

a) 打开 Chrome 的同步功能。
b) 登录一个网站，注册一个账号。
c) 单击密码文本框 -- 建议强密码。
d) 如果没有看到此选项，请右键单击“密码”文本框，然后单击“生成密码”。
e) 你将看到密码的预览。要确认，请单击“使用建议密码”。
f) 完成注册后，你的密码会自动保存到 Chrome 中。

获得最新的官方操作指南，请访问
https://support.apple.com/guide/iphone/create-website-and-app-passwords-iphf9219d8c9/ios

在 iPhone 上创建网站和应用程序密码

a) 在网站或应用程序的新帐户屏幕上，输入一个新的帐户名称。
b) 对于支持的网站和应用程序，iPhone 会提供一个独特而复杂的密码。
c) 请做以下事情之一：
   - 选择建议的密码：点击使用强密码。
   - 设置你自己的密码：点击选择我自己的密码。
d) 如果要让 iPhone 自动为你填写密码，当你被问到是否要保存密码时，点击是。

统一资源定位符 （URL）

统一资源定位符 (URL)，通俗称之为网址，是对网站资源的引用，它指定它在计算机网络上的位置和检索它的机制。

主题：如何保护密码不会泄漏？

1）不要点击未经请求的信息中的链接或附件。最好是直接在浏览器中输入网址，以避免被带到钓鱼网站。

2）使用双因素身份验证。越来越多的在线服务提供商通过要求用户输入一次性密码和普通密码来保护你的账户。

3）密切关注你不同账户中任何可疑活动，如果你发现任何异常，请立即与供应商联系。

4）其他安全技巧：

a）不要与其他人或其他系统共享密码

b）不要使用共享电脑或笔记本电脑

c）谨慎在咖啡馆用手机链接免费无线，银行并不安全

d）不要把你的密码写在便利贴上，也不要把它存在你手机上不安全的备忘录里

e）不要将列表保存在笔记本电脑上未受保护的文档、文本文件或电子表格中

f）避免在多个网站上使用相同的密码：你可能会一次性泄露所有的账户。

主题：如何保护我的生物特征信息？

生物识别标识是独特的、可测量的特征，用于标签和描述个人。生物识别通常被分为生理特征和行为特征。生理特征与身体的形状有关，包括但不限于指纹、手掌静脉、脸部识别、DNA、掌纹、手部几何、虹膜识别、视网膜和气味。行为特征与一个人的行为模式有关，包括但不限于打字节奏、步态和声音。一些研究人员已经创造了术语行为计量学来描述行为特征。

1）强密码：通过简单地破解你的密码来窃取你的数据是比较困难的。不要将你的生物特征保存在很多地方，少数几个地方就可以，这样可以很大程度上防止黑客窃取你的数据。

2）及时将软件更新到最新版本：当你的设备制造商通知你一个可用的软件更新或补丁，请立即安装，这样可以帮助减少你的设备受到安全威胁的可能性。保持你的操作系统和安全软件的更新到最新版本十分重要。

3）选择不提供生物识别标识：如果你担心你生物识别数据的安全，有时你可以选择不提供该数据。可以考虑不需要指纹认证或者不使用面部识别软件的智能手机，也可以在应用程序的设置中禁用面部识别。

4.2 公共设备的安全问题

级别	认识 / 提高警觉 / 保护自己
相关用户	学生、家长、老师
相关隐私	个人身份信息，网络身份信息
风险	用户信息泄露

如果你遵守一些简单的规则，图书馆、网吧和机场的公共计算机也是安全的。

主题：如何安全使用公用电脑?

1) 不要保存你的登录信息

点击“登出”按钮来登出。仅仅关闭浏览器窗口或者输入其他地址是不够的。

许多程序（特别是社交网站、基于网络的电子邮件和即时通讯系统）都有自动登录功能，可以保存你的用户名和密码。禁用此选项，这样在使用完计算机后，没有其他人可以像你一样登录。

2) 屏幕上有敏感信息时不要让电脑处于无人看管的状态

如果你不得不离开公用计算机，请注销所有程序并关闭所有可能显示敏感信息的窗口。

3) 清除你的痕迹

Internet Explorer 11 提供隐私保护浏览模式，不会留下任何特定网页活动的痕迹。如果你不选择该浏览，即使你已经关闭并注销了，浏览器还是会记录下你的密码和你访问的每个页面。

4) 禁用存储密码的功能

在开始浏览网页之前，关闭 IE 浏览器的记忆密码功能。

a) 在 Internet Explorer，点击“工具”，然后点击“互联网选项”。

b) 点击“内容”标签，然后点击“设置”，旁边的“自动完成”。

c) 单击此处可清除与密码有关的两个复选框。

5) 删除你的临时网络文件和浏览历史

当你使用完公共计算机后，可以通过删除临时 internet 文件来帮助保护你的私密信息。

6) 注意偷窥

当你使用公用电脑时，要当心窥视者，窥视者会从你的肩膀后面窥视你，或者站得离你特别近，以便记下你的敏感信息（如密码）。

7) 不要在公用电脑上输入敏感信息

上述措施可以一定程度上防止在你使用完公用电脑后，有黑客也使用这个电脑，从而窃取你的信息。

但是一个非常狡猾的黑客可能已经在公共电脑上安装了复杂的软件，记录下每一次点击，然后通过电子邮件将这些信息反馈给他。

那么，即便你没有保存你的信息，或者你已经删除了你的痕迹，他们仍然可以获得这些信息。

如果你想要真正的安全，避免在公共电脑上输入任何敏感信息，特别是你的信用卡号码或任何其他个人或财务信息。

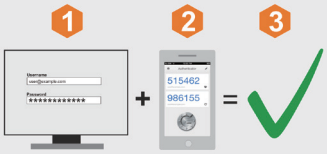
扩展阅读

United Nations
Educational, Scientific and
Cultural Organization

1) 关于联合国教科文组织信息系统的信息通信技术安全手册

信息安全的基本概念和保护自己的一般技巧。

链接：http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/ERI/pdf/ICTSecurityBooklet_En.pdf



2) 双因素认证提供了针对各种攻击的安全性。

第二个身份验证因素可能带来一些不便，但是它极大地提高了安全性。

链接： https://www.welivesecurity.com/2019/12/13/2fa-double-down-your-security

RSA CONFERENCE

3) 不启用 MFA （也通常称为双因素身份验证）的风险

超过 99.9% 的被攻击者入侵的微软企业账户没有使用双重身份验证。本课程将描述微软实现 100% 补救的危险和惊喜，并提供实用的指导来帮助你。

链接： https://v.qq.com/x/page/x01542hoddr.html

4) 创建一个长而复杂的强密码。

密码通常是保护我们个人和财务信息的第一道防线。该“一分钟”指南可指导你如何创建一个长而复杂的强密码。

链接 : https://v.qq.com/x/page/l0531h37l37.html

第五章 在线学习平台中的数据和隐私安全

学习者登录学习平台后，可以报名参加课程，在论坛、博客上发布信息，浏览和学习课程内容。本节介绍在线学习过程中与个人数据保护相关的事项。

学习管理系统 (LMS)

学习管理系统（Learning Management System，LMS）是一种用于管理、记录、跟踪、报告、提供教育课程、培训项目或学习发展项目的软件应用程序。

– Ellis, Ryann K. (2009), Field Guide to Learning Management, ASTD Learning Circuits, archived from the original on 24 August 2014, retrieved 5 July 2012

联合国教科文组织推荐的数字学习管理系统：

- CenturyTech- 运用微课程发展个人学习路径，以解决知识的差距，挑战并促进学生的长期记忆力。
- ClassDojo- 将教师、学生和家长联系起来，建立课堂社区。
- Edmodo- 提供多种语言的能够远程管理教室和吸引学生的工具和资源。
- Edraak- 为学校学生和教师提供阿拉伯语在线教育资源。
- Ekstep- 拥有丰富学习资源，提供识字和算术指导的开放学习平台。
- Google Classroom- 帮助班级进行远程连接，沟通和组织管理。
- Moodle- 社区驱动和全球支持的开放学习平台。
- Nafham- 阿拉伯语在线学习平台，提供与埃及和叙利亚课程相对应的教育视频课程。
- Paper Airplanes- 将个人与私人教师配对，通过视频会议平台，提供英语和土耳其语两种语言的 12-16 周的课程。
- Schoology- 支持教学、学习、评分、协作和评价的工具。
- Seesaw- 支持创建能够在线协作和共享的学习档案和学习资源。
- Skooler- 将 Microsoft Office 软件转化为教育平台的工具。

5.1 课程注册与管理

级别	认识 / 提高警觉 / 保护自己
相关用户	学生、家长
相关隐私	基本信息，出勤信息，偏好，学习记录
风险	由于用户、站点或第三方造成的数据泄漏。

课程注册和管理是在线学习系统提供的基本功能。通过报名参加一门课程、一个班级或者一个小组，你可以更方便、更有效地管理你的学习进程以及与他人进行交流。

主题：如何报名参加课程？（以 Coursera 为例）

1) 报名参加一个课程

a) 点击课程目录中的课程标题，打开课程详情页。

b) 点击注册按钮。

c) 按照说明报名参加课程。可以选择免费试用。

2) 查看报名的课程

你可以在 Coursera 的主页上查看你注册的所有课程，具体操作步骤：

a) 打开 Coursera 官网，确保你已经登录。

b) 在左侧栏中，单击注册课程。

c) 找到“我的课程”部分，查看你注册的课程。

主题：如何浏览和关注社区 ?(以 Edmodo 为例)

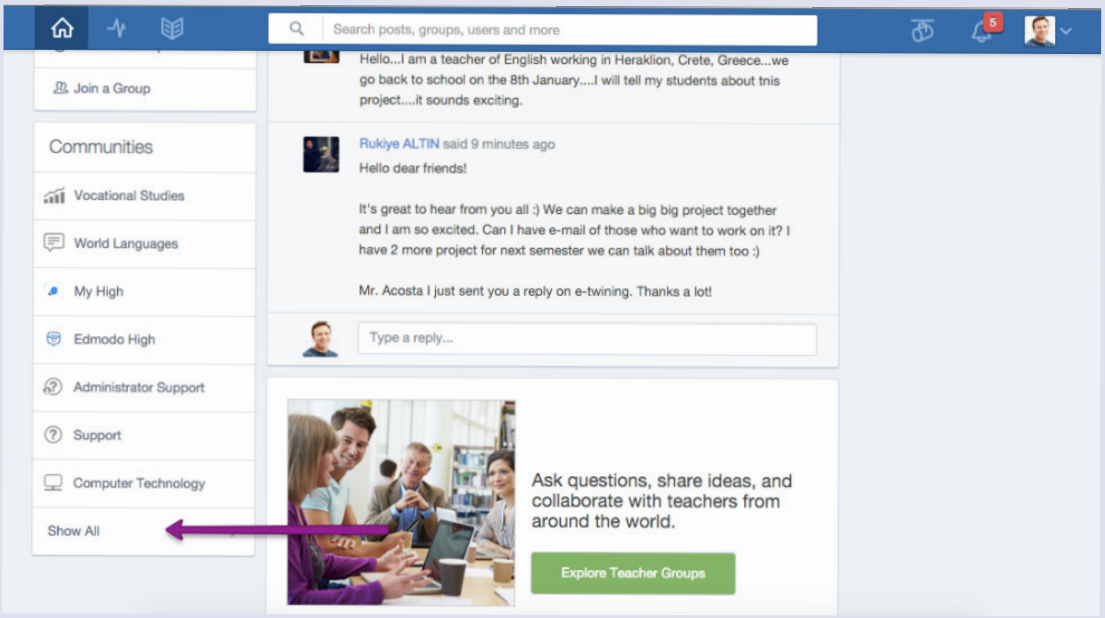
首先，按照以下步骤浏览社区，然后按照你感兴趣的步骤进行操作。

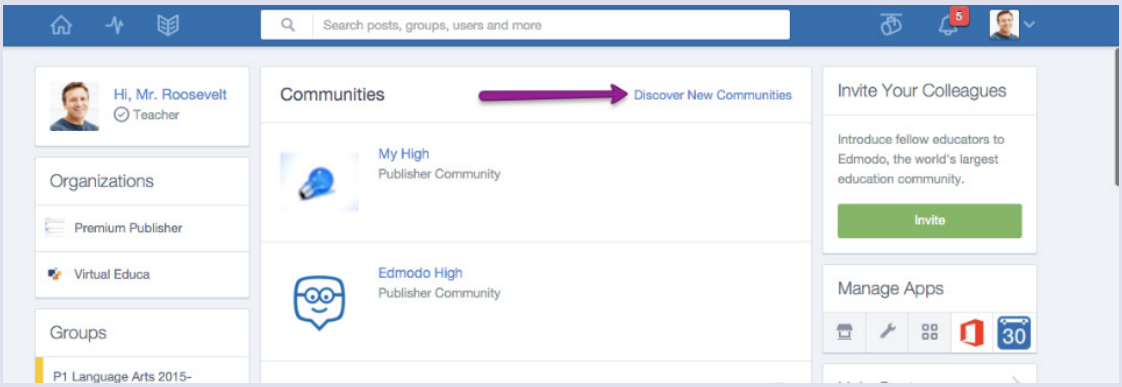
a) 在主页左侧面板的“社区”部分，点击“全部显示”。

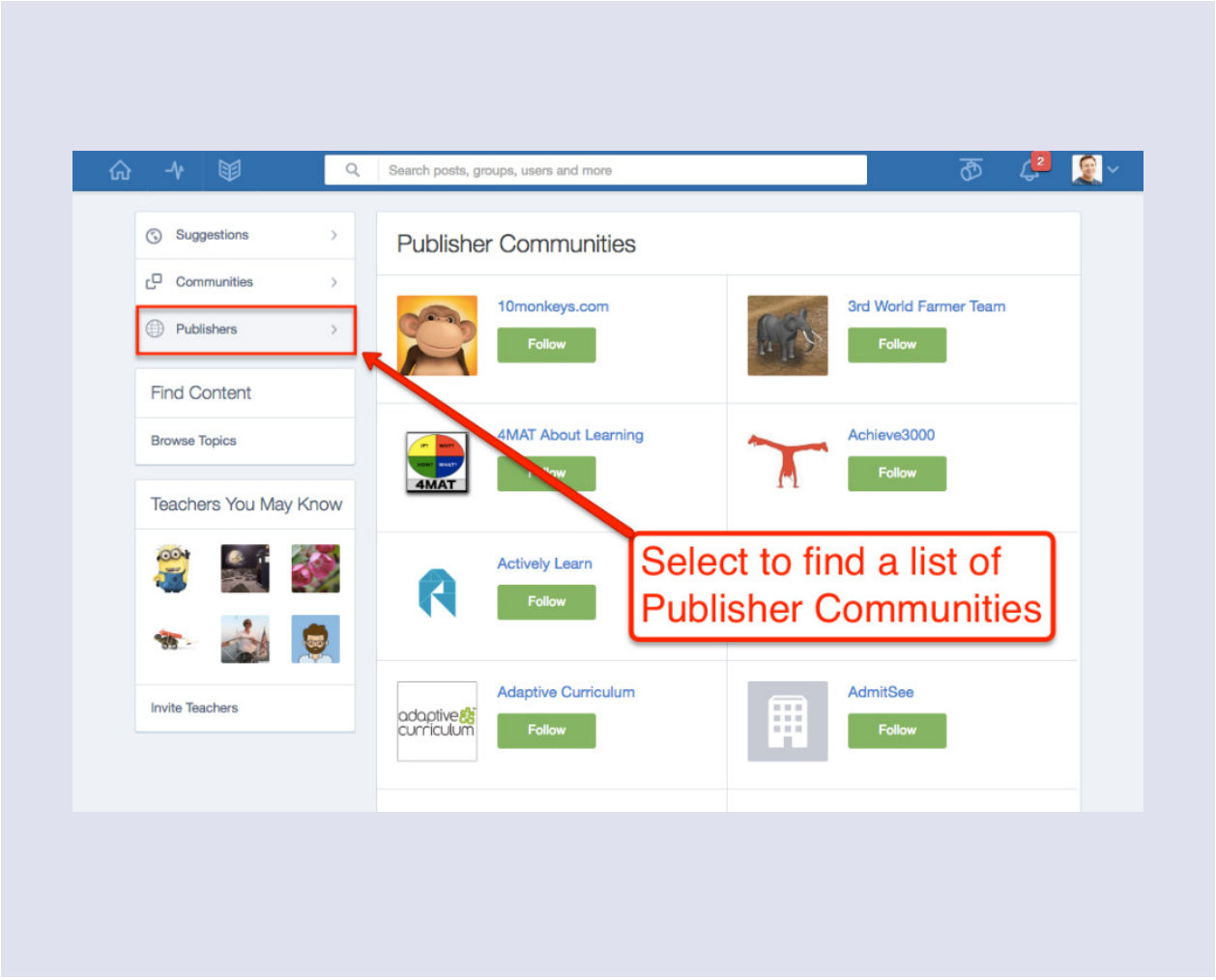
b) 点击右上角的“发现新社区”可以查看所有社区。

c) 直接在此页面上单击“关注”以关注发布者，按钮字样会变为“已关注”。或者，你可以单击发布者页面以查看活动，然后单击页面左侧面板上的绿色“关注发布者”按钮。按钮字样也会变为“已关注”。

d) 通过点击 Edmodo 页面左侧面板和主页中的“社区”来查看你正在关注的社区帖子。







5.2 个性化学习服务

级别	保护自己
相关用户	学生
相关隐私	个人上网记录
风险	· 提取和恶意使用信息，如用户偏好和学习模式等 · 由于平台受到外部攻击而导致用户信息泄露 · 向第三方平台提供非法信息

个性化学习是一种教育方法，旨在根据每个学生的长处、需求、技能和兴趣定制学习。个性化学习有很多潜力，但也有一些风险，个人数据安全是个性化学习的基础。

主题：教育管理者在制定各种个性化学习策略时需要知道什么？

1) 保证对数据的访问

教师、家长和学生都需要及时获得所需的数据，以了解学生的需求，设定更为合适的学习目标，并观察学生如何朝着这些目标前进。

2) 使数据的使用成为可能

教师需要接受相应的培训，以了解如何分析、保护和使用数据，以及确定分析、计划和同伴协作的合适时机。

3) 保护学生数据的隐私

只有当隐私保护措施到位，并且每个使用数据的人都知道他们在保护数据方面所起到的作用时，这种方法才会奏效。

5.3 使用搜索服务

级别	保护自己
相关用户	学生
相关隐私	网络浏览痕迹
风险	· 提取和恶意使用信息，如用户偏好和学习模式 · 由于平台受到外部攻击而导致用户信息泄露 · 向第三方平台提供非法信息

当你在线学习时，可能会经常在网上搜索。然而，搜索有时候可能会使你的隐私受到威胁。在搜索时你需要注意并保护自己的隐私。

搜索引擎

搜索引擎是指根据一定的策略、运用特定的计算机程序从互联网上采集信息，在对信息进行组织和处理后，为用户提供检索服务，将检索的相关信息展示给用户的系统。搜索引擎是工作于互联网上的一门检索技术，它旨在提高人们获取搜集信息的速度，为人们提供更好的网络使用环境。

主题：如何保护你的搜索隐私？

当你使用非个人的电脑，如公用电脑时，记住不要泄露你的个人信息。

1) 不要把个人识别信息放在你的搜索词中

不要搜索你的姓名、地址、信用卡号码、社会保险号码或其他个人信息。这些类型的信息搜索会让你暴露在身份盗窃和隐私侵犯的风险之中。

2) 及时清理和删除你的搜索记录

可以使用浏览器提供的历史记录清理功能，也可以通过搜索引擎提供的在线账户提供的搜索活动管理功能来管理你的搜索记录，以及决定搜索引擎是否有权收集你的上网记录。

HTTP cookie

HTTP cookie（也称为 Web cookie，Internet cookie，browser cookie 或简称 cookie）是从网站发送并在用户浏览时由用户的浏览器存储在用户计算机上的一小段数据。

主题：如何屏蔽搜索引擎中的 cookies？

从隐私保护的角度来看，最好屏蔽所有 cookies。然而，由于 cookies 是访问许多网站所必需的，允许短暂的“会话”cookies 可能更方便（尽管减少了对隐私的保护）。这些 cookie 仅在你的浏览器处于打开状态时才有效。因此，如果退出浏览器，重新打开浏览器，然后返回搜索引擎，则搜索提供程序将无法通过 cookie 将当前搜索与以前的搜索连接起来。

使用以下步骤只允许“会话 cookie”，并记住每天至少关闭一次浏览器，但最好是在每次访问搜索提供的网站之后。在使用 Firefox 时可以进行如下设置：

a) 在编辑功能表中，选择偏好设定
b) 点击隐私
c) 选择 cookie 标签
d) 将保留 cookie 设置为直到我关闭 Firefox

5.4 管理定位服务

级别	认识 / 提高警觉 / 保护自己
相关用户	学生
相关隐私	个人位置资料
风险	· 位置 / 信息泄露对人身和财产安全的威胁 · 由于平台受到外部攻击而导致用户信息泄露 · 向第三方平台提供非法信息

你的手机或电脑中的许多应用程序都会索取你的位置信息。然而，对其滥用可能会造成个人信息泄露。你应该知道如何保护你的位置信息不被盗取。

位置服务 (LBS)

基于位置的服务 (LBS) 是一个通用术语，表示利用地理位置数据和信息向用户提供服务或信息的软件服务。LBS 可以应用于多种场合，如健康、娱乐、工作、个人生活等。

主题：如何防止手机被追踪?

a) 关掉手机上的蜂窝网络和无线网络。完成这项任务最简单的方法是打开“飞行模式”功能，使设备无法连接到网络。

b) 关闭手机的卫星定位服务。一些手机将其作为独立设置，而另一些手机则将其捆绑到隐私或位置设置等菜单中。关闭手机上的基于位置的功能可以防止其被激活，从而防止它提供你手机的位置。

c) 在 iPhone 上：进入你手机的设置，然后选择隐私，再从这里选择定位服务。你会看到一系列使用位置服务的应用程序，可以选择通过移动顶部的滑块来禁用它们，或者只禁用特定应用程序的位置服务。

d) 在安卓手机上：不同的手机可能会有区别，可以打开设置，在搜索框中搜索“定位”、“隐私”等关键词，来进行相关的设置。

5.5 备份个人数据

级别	认识 / 提高警觉 / 保护自己
相关用户	学生，家长，老师
相关隐私	个人身份信息等
风险	· 转售个人资料 · 广告 · 生命安全

当你的电脑受到恶意软件攻击时，可能会导致你的文件丢失和损坏，这将影响你的学习、工作和生活。以下是一些备份系统的方法，以防类似的情况发生。

主题：如何进行数据备份？

对整个系统进行备份是对付硬件故障、软件问题（比如升级）和恶意软件的最佳策略，这些恶意软件不仅会破坏系统，还会破坏文件。

1) 数据备份到硬盘

如果你的空余磁盘上有足够的容量，你可以将数据备份到上面。这些备份既快捷又方便，而且不需要网络。在 Windows 上的操作是设置—更新和安全—备份，在 macOS 上可以使用时间机器应用程序。

2) 备份到云存储

磁盘备份的现代化替代方案是云存储。使用这种类型的解决方案，你可以在云供应商或服务提供商的数据中心中订阅特定的存储容量。与磁盘驱动器不同，你不需要任何硬件，但是需要互联网连接将备份发送到云端中。

拓展阅读

1) 利用学生智能手机进行学习的六种方法

正如 ISTE 教育标准所拥护的那样，智能手机为教师提供了一种简单的方式来“促进和激发学生的学习和创造力”，同时也增加了学生的积极性。以下是使用学生智能手机学习的六种方法。

链接：https://www.iste.org/explore/toolbox/6-ways-use-students-smartphones-learning

2) 联合国教科文组织免费提供在线课程

为了保证学习的连续性，在教科文组织内罗毕办事处主任的全面协调下，科学部门汇编了各种教育资源，以帮助非洲大陆的学生，特别是来自脆弱和贫穷社区的学生。

这些教育资源涵盖多个学科范畴，包括自然科学、数学、工程学、文科、社会科学等以满足学生的需要。

链接： https://zh.unesco.org/sites/default/files/overview_of_e-learning_materials_0.pdf

3) 在线学习的有用工具

下面的网站展示了一些最好的在线学习工具，分别用于教师的混合学习，翻转课堂和远程学习模型。

链接：https://www.educationworld.com/a_tech/favorite-tools-for-online-learning.shtml

4) 终身学习者教育网站

下面的网站提供了历史、经济、科学和哲学领域不同类型教育资源的网站列表，包括书籍、视频、音频和课程。

链接：https://medium.com/@imaginetta/150-educational-web-sites-for-lifelong-learners-71c1d8e94843

第六章 社交网络工具中的数据和隐私保护

社交网络正越来越多地用于在线学习。它提供一种媒介，使学生们能够积极主动地进行多人协作，并与教师共同创造知识和分享经验。然而，社交网络的过度使用可能会对学生的学习生活产生负面影响，例如：个人信息泄露，注意力分散，以及过度沉迷。

社交网络和社交网络服务

社交网络是一种社会结构，由一组社会行为者 (如个人或组织)、一组二元关系以及行为者之间的其他社会互动组成。社交网络视角为分析整个社会实体的结构提供了一套方法，同时也提供了各种理论来解释这些结构中所观察到的模式。

– Wasserman, Stanley; Faust, Katherine (1994). “Social Network Analysis in the Social and Behavioral Sciences”. Social Network Analysis: Methods and Applications. Cambridge University Press. pp. 1–27. ISBN 9780521387071.

社交网络服务 (也包括社交网站或社交媒体) 是一个在线平台，有着相似的个人或职业兴趣、行为、背景或现实生活中的联系的人们可以利用这个平台与其他人建立社交网络或社交关系。

6.1 使用视频会议工具

级别	认识 / 警惕 / 保护自己 / 保护他人
相关用户	学生、家长、老师
相关隐私	个人身份信息，个人财产信息，个人位置信息
风险	· 包含个人可识别信息，个人位置信息，个人财产信息等的实时图片 · 由于平台受到外部攻击而导致用户信息泄露 · 由于个人设备受到外部攻击，用户遭到信息泄露攻击

利用视频会议工具进行在线研讨正逐渐成为网络时代学术交流、工作和学习的重要手段。建议考虑以下建议，安全使用这些软件。

主题：在线直播时确保网络安全—给家长和监护人的建议

1) 经常与子女交谈

经常与你的孩子沟通，了解他们的数字生活和如何使用在线服务。

2) 在开始直播前，确保个人信息安全

确保你的孩子了解直播的风险。直播不能被编辑，也不能抹去人们已经看到的东西。提醒他们，个人信息可能会通过在直播中说的话、甚至是环境背景中的东西泄露出去。其他人可以保存直播录像并大肆传播。

3) 限制子女使用设备和网络服务

如果一个网站有隐私设置，了解这些设置并确保哪些人可以 / 不可以联系你的孩子。

家长可以制定一个家庭协议，在这个协议中，家庭成员都可以承诺是否使用直播服务，谁可以一起使用这些服务，或者在家里哪里位置可以使用这些服务。家长应决定用于直播和视频聊天的设备（如平板电脑、手机、网络摄像头）不应放在卧室或更私密的地方。

4) 教你的孩子什么时候说不

儿童可能被强制训练或胁迫在摄像机前裸露或相关行为。这些内容可能会被恶意记录和违法传播，用来威胁或勒索少年儿童。因此，家长和监护人必须了解儿童使用在线服务的情况，并让他们了解潜在的危险。

告诉你的孩子，如果他们被要求在网上说或做一些觉得不舒服的事情，他们可以拒绝，并结束聊天或视频直播，同时和家人或其他值得信任的成年人交流。应该提醒孩子们，及时告诉家长在网上发生的事情。

5) 举报辱骂性内容

教会孩子如何举报攻击性或辱骂性的内容。你可以使用常用平台上提供的相关功能，或从其提供的隐私政策中找到更多有用信息。

你也可以直接登录中央网信办违法和不良信息举报中心网站 https://www.12377.cn/ 或拨打 12377 进行举报。

联合国教科文组织建议的支持实况视频通信的协作平台：

- 钉钉—交流平台，支持视频会议，任务和日历管理，出勤记录和即时通讯
- Teams—聊天，会面，电话和协作功能，集成微软 Office 软件
- Skype—视频和音频通话与谈话，聊天和协作功能
- 腾讯会议—内容分享和视频 / 音频会议工具，最大可容纳 300 名参加者
- Zoom—视频和音频会议、协作、聊天和网络研讨会的云平台

6.2 发布网络信息内容

级别	认识 / 警惕 / 保护自己 / 保护他人
相关用户	学生、家长、老师
相关隐私	个人身份信息，个人财产信息，个人信息位置
风险	· 提取和恶意使用信息，例如用户偏好 · 由于平台受到外部攻击而导致用户信息泄露 · 向第三方平台提供非法信息

你可以发布一些东西，比如文本、照片、视频或者网站链接。一旦发布，在某种程度上，你无法控制其传播和造成的影响，所以在网上发布时要小心。

主题：社交网络中的基本注意事项

无论是使用网络交友平台，还是仅仅在线上聊天，你都有可能把个人信息泄露到网上。你无法控制它会造成什么后果，而这可能会对你的隐私构成风险，甚至有身份盗窃或网络诈骗的风险。

避免与其他人分享太多的个人信息，例如限制陌生人访问你的社交媒体页面。花点时间了解一下你最喜欢的社交网络平台的隐私政策和隐私设置并善加利用。

当你在网上发布信息和内容之前，不妨考虑以下几件事：除了你的目标受众之外，还有谁可能会看到这些信息？你写的东西或者你发布的图片会在现实生活中引起尴尬吗？如果你现在或者未来的雇主看到你发布的东西，你会有什么感觉？

主题：注意网络礼仪

1) 注意发布的内容

避免发布尴尬、暴露或负面的照片。你分享的照片可能可能被认为是你的表象，或者反映了你的性格。在高中或大学里看起来可爱的东西，对于潜在的雇主来说可能并不那么可爱。

不要在网上透露个人隐私，包括生日、电话号码、地址、学校等。不要泄露你的常去地点或者何时不在家中。

2) 语调和态度

专业精神是必不可少的：如果你在工作场合不会这么说，那就不要在网上这么说。

礼貌和尊重是至关重要的：体谅他人，以你希望别人对待你的方式来对待他们。

错别字、标点符号错误、语法和遣词造句不恰当会带来不好的影响：发送前要进行校对，避免不恰当地使用缩写和网络俚语。

3) 做一个负责任的用户

了解各种在线论坛（社交网络、博客、在线社区）的行为准则和互动方式。

发布涉及他人信息的帖子时，考虑你的行为会给别人造成的后果和留下的印象。

善于使用隐私设置来限制谁可以查看和分享你的个人资料和发帖记录。

当你要添加一个不认识你的人成为在线好友时，详细解释你是谁以及你为什么要添加他们。

6.3 屏蔽不健康内容

级别	认识 / 提高警觉 / 保护自己
相关用户	学生
相关隐私	个人上网记录
风险	· 提取和恶意使用信息，例如用户用户偏好 · 由于平台受到外部攻击而导致用户信息泄露 · 向第三方平台提供非法信息

在开始一门课程之前，学生们最好浏览一下自己感兴趣的东西。在这个阶段，确保内容合适是至关重要的。

主题：如何屏蔽不适当的内容?

1) 在 Windows10 上

获得最新的官方操作指南，请访问 https://support.microsoft.com/zh-cn/help/12413/microsoft-account-what-is-family-group

当你使用 Internet Explorer 和 Microsoft Edge 浏览器时，可以在 Xbox One 和 Windows 10 设备上阻止不适当的网站。若要打开 Web 浏览，请转到 https://account.microsoft.com/family，然后使用你的 Microsoft 帐户注册。然后：

a) 查找子女的姓名，并选择“内容限制”。

b) 向下滚动到“Web 浏览”，然后将“阻止不适当的网站”从“关”切换为“开”。

c) 如果你想要始终阻止特定站点，请在“始终阻止”下方添加其 URL。

d) 如果你希望子女仅查看你明确允许的网站，请选中“仅允许这些网站”旁的复选框。

2) 在 Mac 上

要获得最新的官方操作指南，请访问

https://support.apple.com/guide/mac-help/welcome/mac

a) 在 Mac 上，请执行以下一项操作：

- 如果使用“家人共享”登录你的 Mac 用户帐户，然后确保已使用 Apple ID 登录。
- 如果未使用“家人共享”：登录子女的 Mac 用户帐户。

b) 选取苹果菜单 > “系统偏好设置”，然后点按“屏幕使用时间”。

c) 如果使用“家人共享”，请点按边栏中的弹出式菜单，然后选取子女。

d) 点按边栏左下角的“选项”。

e) 点按右上角的“打开”。

f) 选择以下任一选项：

- 包含网站数据：如果想要“屏幕使用时间”报告包括所访问特定网站的详细信息，请选择此选项。如果不选择此选项，所访问的网站只会报告为 Safari 浏览器使用时间。
- 为屏幕使用时间设置密码：选择此选项以防止更改“屏幕使用时间”设置，并在达到限额时要求输入密码以允许更多使用时间。

3) 在 iPhone 上

要获得最新的官方操作指南，请访问

https://support.apple.com/guide/iphone/welcome/ios

在 iOS 13.3、iPadOS 13.3 或更高版本中，你可以始终阻止或在特定时段内阻止家庭成员设备上与特定联系人的双向通信，包括电话、FaceTime 通话和信息。

a) 如果还没有在家庭成员的设备上打开 iCloud 中的“通讯录”，请前往“设置” > [孩子的姓名] > iCloud，然后打开“通讯录”。

【注】只有家庭成员使用 iCloud 中的“通讯录”时你才能管理其通信。

b) 在家庭成员的设备上，前往“设置” >“屏幕使用时间”。

c) 如果还没有打开“屏幕使用时间”，请轻点“打开屏幕时间”，轻点“继续”，然后轻点“这是我孩子的 iPhone”。

d) 轻点“限定通信”，然后执行以下任一项操作：

- 随时限定通信：轻点“在屏幕使用时间内”，然后选择“仅限联系人”、“联系人及包含至少一位联系人的群组”或“所有人”。
- 停用期间限定通信：轻点“停用期间”。“在屏幕使用时间内”中所选的选项已在此处设定。你可以将此设置更改为“特定联系人”。
- 如果选择“特定联系人”，之后请轻点“从我的联系人中选取”或“添加新联系人”以选择要在停用期间允许与其通信的联系人。
- 管理孩子的通讯录：如果使用了“家人共享”，你可以查看、编辑孩子的通讯录，以及在其中进行添加或删除操作。轻点“管理 [孩子的姓名] 的通讯录”。

  如果孩子在 iCloud 中已有通讯录，其设备上会收到通知，要求批准通讯录管理请求。如果孩子没有通讯录，则不会收到通知，你可以立即添加联系人。

  管理孩子的通讯录时，“管理 [孩子的姓名] 的通讯录”下方会新建一行，显示孩子有多少联系人。轻点该行以查看和编辑联系人。
- 允许编辑联系人：轻点“允许编辑联系人”以关闭此选项，并阻止孩子编辑其联系人。

关闭联系人编辑和随时将通信限定为“仅限联系人”能让你很好地控制孩子的通信对象和可通信时间。

如果当前被“限定通信”设置阻止的用户尝试呼叫家庭成员（通过电话或 FaceTime 通话）或者向家庭成员发送信息，其通信不会接入。

如果家庭成员尝试向当前被“限定通信”设置阻止的用户拨打电话或者发送信息，对方的名字或号码会显示为红色并带有沙漏图标，通信也不会接通。如果限制仅应用于停用时间，家庭成员会收到“时间限制”信息，并可在停用时间结束后恢复与该联系人的通信。

若要允许家庭成员与被“限定通信”设置阻止的联系人的通信，请按照上述步骤更改设置。

4) 在安卓手机上

要获得最新的官方操作指南，请访问

https://support.google.com/googleplay/answer/1075738?hl=zh-Hans

a) 在你希望开启家长控制功能的设备上，打开 Play 商店应用 。

b) 点按左上角的“菜单”图标 > 设置 > 家长控制。

c) 开启家长控制。

d) 创建 PIN 码。这样可防止不知道 PIN 码的人更改你的家长控制设置。如果要在孩子的设备上设置家长控制功能，请选择他们不知道的 PIN 码。

e) 点按你要过滤的内容类型。

f) 选择如何过滤或限制访问权限。

设置家长控制功能后，你可以将其开启或关闭。重新开启家长控制功能并创建新的 PIN 码后，你原来的设置就会启用。这样可以方便你与不需要家长控制的人共用设备。

5) 在谷歌浏览器上

要获得最新的官方操作指南，请访问

https://support.google.com/families/answer/7087030?hl=zh-Hans

如果你屏蔽了某个网站，你的孩子可以请求家长同意访问该网站。这时你会在 Family Link 应用中收到通知，并可在应用中批准或拒绝其请求。

- 网站：如果你屏蔽或允许访问特定网站，如 www.baidu.com，则该权限不适用于开头或结尾与此不同的网站，如 news.baidu.com。
- 域名：如果你屏蔽或允许访问整个域名，如 google，则该权限还适用于开头或结尾与此不同的网站，如 www.google.com 和 images.google.fr。

(1) 屏蔽或允许访问网站

a) 打开 Family Link 应用

b) 选择你的孩子。

c) 在“设置”卡片上，点按管理设置 >Google Chrome 上的过滤器 > 管理网站 > 已批准或已屏蔽。

d) 点按右下角的“添加例外情况”图标 添加例外情况。

e) 添加网站（如 www.baidu.com）或域名（如 baidu）。如果你要添加网站，则应该将 www. 部分包含在网址中（如 www.baidu.com 而不是 baidu.com）。

f) 点按左上角的“关闭”图标 关闭。

提示：你也可以通过访问 families.google.com 并点击孩子的姓名来管理孩子的帐号。

域名系统 (DNS)

域名系统 (Domain Name System, DNS) 是互联网的一项服务。它作为将域名和 IP 地址相互映射的一个分布式数据库，能够使人更方便地访问互联网。

(2) 使用安全的 DNS

当用户要访问 www.baidu.com 这样的网站时，用户的计算机需要知道要连接到哪个服务器地址。计算机自身没有相关的信息来完成这种“从名称到地址”的转换，而使用专门的服务器完成这项工作。这个专用服务器称为 DNS 解释器。一些 DNS 解释器可以阻止恶意软件和成人内容。

a) 点击 Chrome 浏览器右上角的⋮

b) 点击设置—隐私和安全性—安全

c) 向下滚动页面，找到“使用安全 DNS”

d) 选择一项 Chrome 提供的 DNS

或“自定义”，这里有一些 Cloudflare 提供的 DNS 地址，可供你的家人使用。

仅阻止恶意软件

主 DNS：1.1.1.2

辅助 DNS：1.0.0.2

阻止恶意软件和成人内容

主 DNS：1.1.1.3

辅助 DNS：1.0.0.3

For IPv6 use：

仅阻止恶意软件

主 DNS：2606:4700:4700::1112

辅助 DNS：2606:4700:4700::1002

阻止恶意软件和成人内容

主 DNS：2606:4700:4700::1113

辅助 DNS：2606:4700:4700::1003

主题：如何管理你的推送通知？

即时获取重要和相关的数据是智能手机在我们生活中如此普遍和流行的原因之一。但是当这些数据较为私人的时候，你不希望它们出现在你的锁屏上让其他人看到。更重要的是，推送式通知可能具有破坏性。通知可能会在不方便的时间到来，或者是彻头彻尾的烦人，或者他们可能会提供不相关的信息，对用户来说没有任何价值。

在 iPhone 上

你可以针对每个 App 自定义大部分通知设置。你可以打开或关闭 App 通知，使通知播放声音，以及选择设备解锁时 App 通知显示的方式和位置等。

a) 前往“设置”  >“通知”。

b) 若要选取想让大多数通知显示预览的时间，请轻点“显示预览”，然后进行选择（“始终”、“解锁时”或“从不”）。（你可以为单个 App 覆盖此设置。）

预览内容可包括来自“信息”和“邮件”的文本，以及来自“日历”的邀请详细信息等。

c) 轻点“返回”，轻点“通知风格”下方的 App，然后打开或关闭“允许通知”。

如果打开“允许通知”，请选取想让 App 通知显示的方式和位置，例如，在锁定屏幕上或在“通知中心”中。

你还可以针对许多 App 设定通知横幅风格、声音和标记。

d) 轻点“通知分组”，然后选取将通知分组的方式：

- 按 App：来自该 App 的所有通知会分组在一起。
- 自动：来自该 App 的通知会使用 App 自带的整理标准分组，如话题或主题。
- 关闭：关闭分组。

若要有选择性地关闭 App 的通知，请前往“设置”>“通知”>“Siri 建议”，然后关闭任意 App。

在安卓手机上

(1) 更改手机的通知设置

重要提示：设置可能因手机而异。如需了解详情，请与你的设备制造商联系。

a) 打开手机的“设置”应用。
b) 依次点按应用和通知 > 通知。
c) 选择要作为手机默认设置的选项：

- 在锁定屏幕上。
- 允许使用通知圆点。
- 默认通知提示音。
- 滑动指纹即可查看通知。
- 勿扰。

(2) 在锁定屏幕上隐藏通知中的敏感内容

重要提示：设置可能因手机而异。如需了解详情，请与你的设备制造商联系。

a) 打开手机的“设置”应用。
b) 依次点按应用和通知 > 通知。
c) 在“锁定屏幕”下，关闭敏感通知。

提示：如果你关闭此选项，则仍然可以限制某些应用在锁定屏幕上“不显示通知”。

主题：应对网络欺凌

网络霸凌是指用短信、邮件、即时消息、社交媒体更新等电子通讯工具来威胁或者侮辱他人。任何年龄的人都可能受到网络霸凌，但青少年是最常见的霸凌对象。网络霸凌的后果和真实生活的霸凌一样严重。网络霸凌永远都不是受害者的错。如果你是受害的当事人，你可以在线屏蔽霸凌的消息，并向当局报告。

1）留意骚扰的迹象。不管你是怕自己受到霸凌，还是担心自己的孩子受到霸凌，留心预警迹象总是能很好地发现网络霸凌。网络霸凌通常是一个人利用邮件、即时消息、短信或者其他电子通讯方式来骚扰另一个人。如果某人直接用以下形式的消息联系另外一个人，那么可以确定这就是网络霸凌：

- 仇恨或者威胁性的消息。这包括恶意称呼、暴力威胁，或者曝光私人信息来控制他人行为的威胁。
- 威胁性的，或者让人尴尬的图片和视频。
- 大量垃圾邮件、即时消息或者短信（不论具体内容是什么）。
- 让人难堪的谎言。

2）留心公开在线侮辱的迹象。另一种常见的网络霸凌是指，霸凌者用公开的方式骚扰他人，而不是和受害者直接联系。网络霸凌者可能会用到公开的策略，比如使用社交媒体、短信或者其它工具传播谣言和八卦。使用在线平台公开侮辱他人的方式还包括：

- 在社交媒体网站、博客或其他公共空间发布侮辱性的消息。
- 在社交媒体网站上，或通过短信分享令人尴尬或者露骨的图片或视频。
- 针对目标，创建满是诽谤性图片、辱骂和谣言的网站。

3）让霸凌者停止他们的行为。有的霸凌者一开始是你的朋友、前任，或者其他你熟知的人。如果不能和他们进行合理的对话的话，直接制止他们的行为。最好当面沟通，不要发邮件或者短信。直白地跟他们说清楚，比如：“我看到你在微博上说我的话了，你不该这么说，你这样伤害了我。我希望你不要再说那样的话。”

- 如果你不知道霸凌者是谁，或者说霸凌你的是一群人，和他们沟通可能就没有用。

4）不要回霸凌者的信息。如果和他们沟通没有用，就不要直接回复他们发来的短信、即时消息、邮件或者其他通讯信息了。霸凌者想要看到你收到消息的反应，所以回复他们的消息只会适得其反。不跟他们接触就是你最好的应对方法。

- 此外，不要威胁或者欺负他们。由于恼怒而发给霸凌者威胁性的信息只会激怒他们，让他们继续他们的恶行，同时也可能让你陷入麻烦之中。

5）把你被网络霸凌的事实告诉一个值得信赖的成年人。如果你是青少年，那就向成年人寻求帮助。你的父母、老师、校长和学校辅导员都有能力在事态发展得更严重之前，制止霸凌。不要期待着这个问题会自己消失。立刻将事情说出来，结束霸凌。

- 你可能很想让霸凌者自生自灭，而不是让更多人关注这个问题。但是如果你这么做，霸凌者们会觉

得骚扰他人不会受到任何惩罚。

6）把你被网络霸凌的事告诉学校的管理人员。把事情的来龙去脉告诉一个有权威的人，然后解释清楚你是如何被网络霸凌的。如果你不想要直接跟校长沟通，告诉你最喜欢的老师或者学校的辅导员。每个学校都有它对付霸凌的政策，越来越多的学校已经针对网络霸凌设置了具体的防治方案。

- 不管学校的具体政策到底是什么，解决这种情况都是学校管理人员的职责。
- 如果你是儿童或者青少年，要明白，把问题报告给学校才是正确的做法。学校中的其他孩子可能也正遭受着网络霸凌。学校需要意识到这个问题，并采取行动制止它。
- 如果你是家长，和学校校长开会直接解决这个问题。

7）把霸凌者举报给服务商或者社交媒体网站。网络霸凌往往违反了社交媒体网站、手机供应商和其他服务商的服务条例。阅读服务商的政策，然后采取行动举报威胁性的行为。服务提供商可能会根据你的举报惩罚霸凌者，或者对他们进行封号处理。

- 你可能需要将网络霸凌者的消息记录发给服务商，证明自己受到了霸凌。

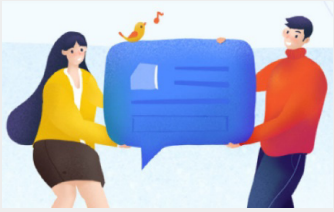
扩展阅读

unicef | for every child

1) 联合国儿童基金会 (UNICEF) 安全返校行动

联合国儿童基金会与中华人民共和国教育部及中国疾病预防控制中心共同启动“安全返校行动”，通过提供实用的信息与指导，帮助孩子安全、健康、快乐地重返校园。

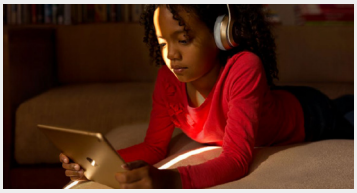
链接： https://www.unicef.cn/covid-19/safe-school-return



2) 腾讯会议操作手册和常见问题

腾讯会议是一个便捷免费的视频会议工具，可以在以下网址找到其操作手册，以及常见的问题解决，如会议声音小、有杂音、如何发起、预定和参加会议等。

链接：https://support.qq.com/products/42324/



3) 苹果家庭

苹果公司推出了一个新的家庭页面，可以帮助家长锁定他们孩子正在使用的 iOS 和 macOS 设备所需的信息。针对智能手机对儿童影响的担忧日益加剧，苹果最近指出，它已经提供了一些工具，帮助父母控制和限制孩子设备上的应用程序、电影、网站、歌曲、书籍、手机数据、密码设置和其他功能。

链接：https://www.apple.com/families/

4) 中国互联网联合辟谣平台

中国互联网联合辟谣平台是由中央网信办违法和不良信息举报中心主办、新华网承办的平台，旨在为广大群众提供辨识谣言、举报谣言的权威平台。

链接： http://www.piyao.org.cn/

中央网信办（国家互联网信息办公室）违法和不良信息举报中心

中央网信办（国家互联网信息办公室）违法和不良信息举报中心统筹协调全国互联网违法和不良信息举报工作；指导、监督各地各网站规范开展互联网违法和不良信息举报工作；受理、协助处置网民对互联网违法和不良信息的举报；宣传动员广大网民积极参与互联网违法和不良信息举报监督；主办中国互联网联合辟谣平台，统筹做好网络辟谣工作；开展国际交流合作，加强与境外国际组织、相关机构、互联网企业的联系，协调处理相关有害信息。

链接：https://www.12377.cn/

第七章 个人信息删除

在完成在线学习一段时间内，用户应注意学习过程中生成的数据，并决定是否删除这些数据。如果你决定删除，这里将提供一些建议和方法。

7.1 删除在线学习数据

级别	认识 / 提高警觉 / 保护自己
相关用户	学生
相关隐私	个人身份信息，个人网络历史
风险	· 该平台不允许删除 · 删除后非法保留信息

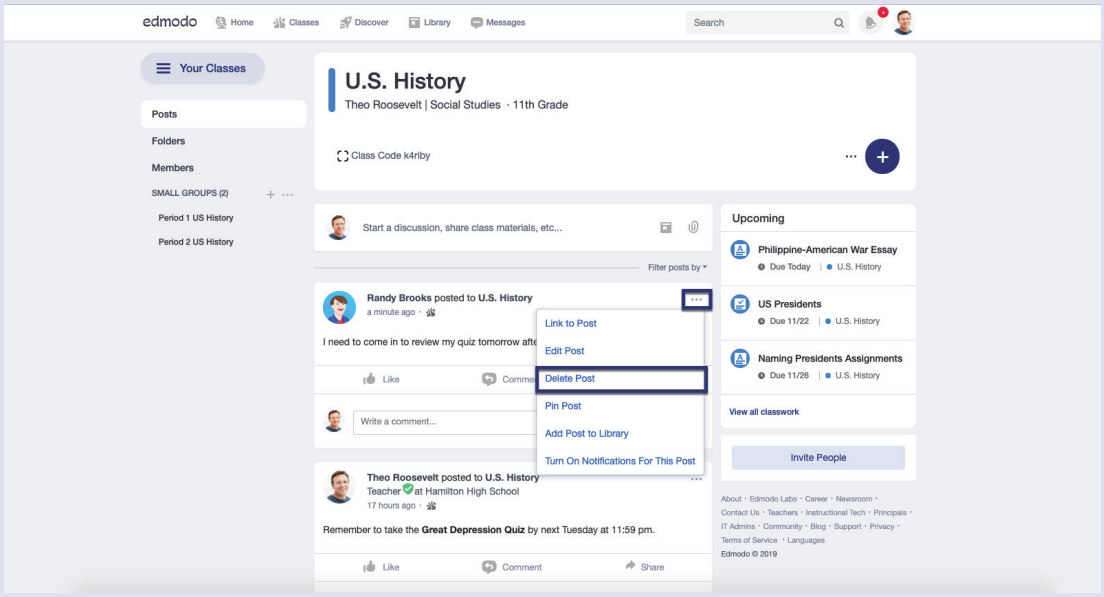
当你不想再继续共享某些内容时，只要你有相应的权限，你可以选择删除它们。下面是在典型平台上删除内容的方法。

主题：如何删除用户生成内容?

1) 在线学习平台 Edmodo

如果你是一名学生，你可以通过以下步骤删除一个帖子：

a) 将鼠标悬停在帖子或回复上，然后点击帖子右上角的「帖子设置」图标。
b) 点击「删除邮件」或「删除回复」
c) 点击「确定」确认。



如果你是一名教师，你可以通过以下步骤删除帖子或评论：

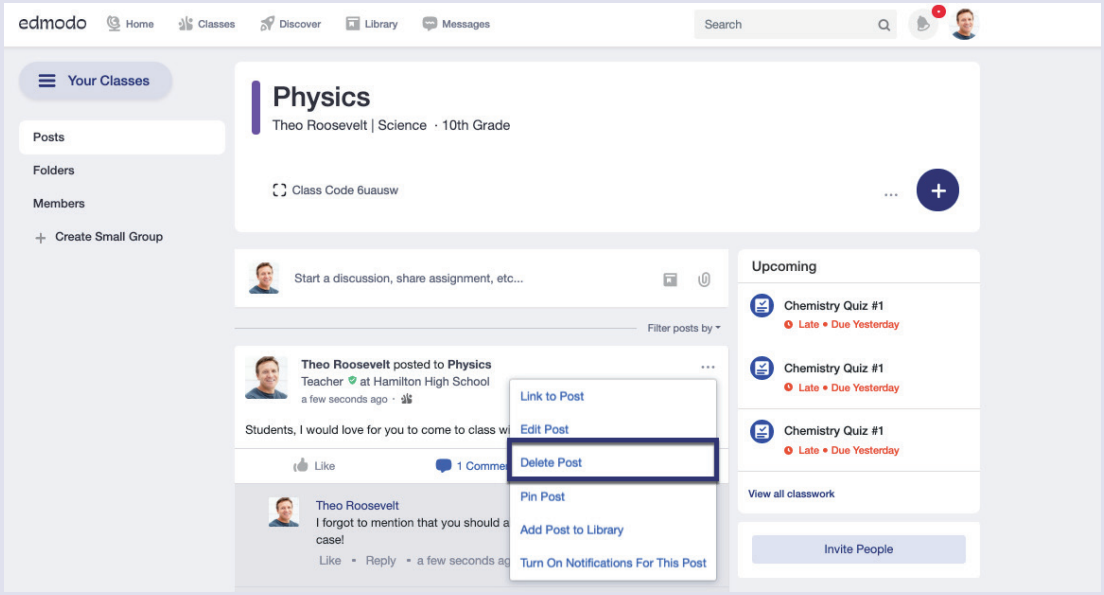
想要删除一个帖子：

a) 找到要删除的帖子

b) 单击文章右侧的「更多」按钮，打开弹出菜单

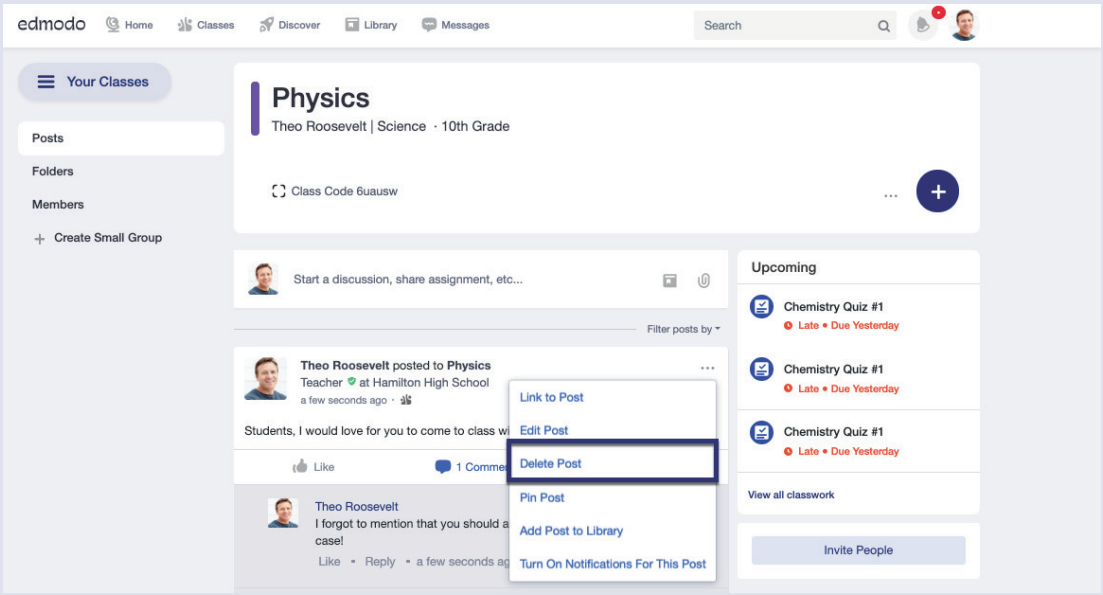
c) 选择「删除帖子」

d) 单击「删除」确认



若想要删除帖子上的评论：

a) 找到要删除的评论
b) 单击注释右侧的向下箭头，打开弹出菜单
c) 选择「删除评论」
d) 单击「删除」确认



2) 在线学习平台 Coursera

如果你想离开组织的学习项目：

当你被邀请通过一个公司或组织参加 Coursera 的学习项目时，你会收到一份你可以拒绝或接受的邀请。

如果你已经在 Coursera 的学习项目中，并且想要注销或者从项目中删除，请与你的企业管理员联系。

如果你想删除社区中的评论或线程：

成员不能自己删除他们的线程 / 帖子，你可以要求社区管理员帮忙删除。

3) 社交网络 - 微博

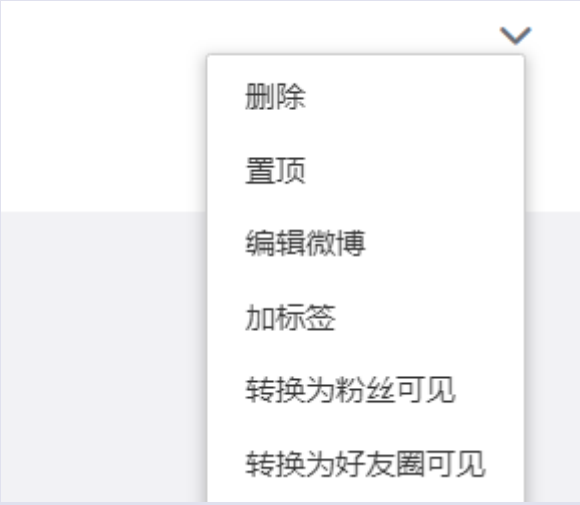
你可以通过以下步骤删除你的微博：

a) 在网页右上角菜单中，点击你的个人资料图标
b) 点击“微博”。

c) 找到你想删除的微博。

d) 在下拉菜单中找到删除选项。

e) 点击“删除”。



7.2 注销账户

级别	认识 / 提高警觉 / 保护自己
相关用户	学生
相关隐私	个人身份信息，个人网络历史
风险	· 该平台不允许停用 · 禁用后非法保留信息

当你不想在学习平台上进行任何活动时，你可以选择关闭或删除账号，这里有一些典型的平台注销方法供你参考。

主题：如何停用帐号？

1) 在线学习平台 Edmodo

你可以通过以下步骤停用你的账号：

a) 点击个人资料图片旁边的帐户图标，然后点击「设置」。
b) 滚动到页面底部，点击「删除账号」。
c) 阅读警告并单击「禁用」。

如果你不能使用以上步骤注销你的帐号：

a) 请从你的学生帐号上的电子邮件地址与我们联系，并选择“错误的帐户类型 / 注销帐户”如果你的学生帐号上没有电子邮件地址，你可以在帐号设置页面上添加一个。
b) 使用命令“删除学生帐号”来要求删除你的帐号。

2) 在线学习平台 Coursera

如果你不想再使用你的 Coursera 账号，你可以选择删除。

如果你只是不想再收到 Coursera 的邮件，你可以更改你的邮件设置。

想要删除你的账号：

a) 登录你的 Coursera 账号
b) 打开右上角的下拉菜单
c) 点击「设置」
d) 单击页面底部的「删除账号」

如果你删除了你的 Coursera 账号，你可能无法恢复你的旧账号信息。需要创建一个新的账号才能再次使用 Coursera。

3) 社交网络 - 微信

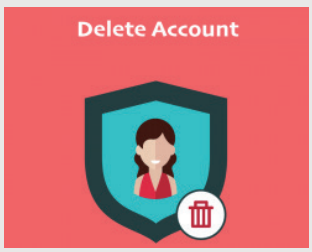
a) 点击右下角的「我」。
b) 在个人资料页，点击「设置」。
c) 在设置页面，点击「账号与安全」，进入微信安全中心。
d) 选择「注销账号」根据提示完成操作即可。

扩展阅读

1) 使用微博新的隐私和数据选项来保护你的账号

以下是微博的隐私保护政策，它可以帮助你更好的维护自己的账号，防止自己的隐私被他人窃取。

链接： https://www.weibo.com/signup/v5/privacy



2) 在你删除任何在线账号之前改变以下 4 个方面

当浏览网络时，人们的第二天性是在各种网站上注册，以便获得各种各样的服务、功能和好东西。一旦问题解决后，你就会转向更新、更吸引人的东西，留下一串未使用的账户。为了享受更好的数字生活，请避免那样的杂乱生活。

链接： https://www.makeuseof.com/tag/make-4-changes-delete-online-account/

3) 如何在安卓系统删除微信

wikiHow 教你如何使用 Android 永久删除你的微信账户和所有聊天记录。

链接：https://www.kafan.cn/A/pv065rg2vd.html

4) 账号删除或禁用 - 如何处理你的旧账号

当你不再使用社交网络的个人资料或网站时，停用或删除你的账户是个好主意。这将意味着你的内容不再存在，不会在网上搜索到；它还将消除这些账户被他人使用或在你不知道的情况下被黑的风险。

链接： https://www.childnet.com/blog/delete-or-deactivate-what-to-do-with-your-old-accounts

5) 如何删除你不需要的账号

拥有太多的数字账户会增加你的数据被滥用或被盗的风险。

链接：https://www.consumerreports.org/privacy/how-to-delete-online-accounts-you-no-longer-need/

结语

在线学习正逐渐成为每个人的基本学习方式，尤其是在新型冠状病毒肺炎流行期间。在线学习的过程中个人信息被大量收集，每个学习者都应确保个人隐私安全。学习者迫切需要掌握保护个人数据和隐私的基本技能。

在这本指导手册中，我们分析了个人数据、隐私、在线学习等几个术语的定义，以及不同国家和国际组织在个人数据保护方面的立法法规。讨论了个人数据、学生数据、学生隐私之间的关系，列出了在线学习中需要遵守的隐私框架和原则，并分析了学生和家长有关在线学习中被收集的数据的权利。

在分析的基础上，这本指导手册确定了以下有关在线学习中如何保护个人数据和隐私的五个方面。

1) 在线学习前准备好设备和工具。在线学习前设置设备、管理网络设置、选择和安装工具，确保良好的学习环境是保障个人数据的基础。手册给出了有关这些问题的多种建议和解决方案。

2) 在登入学习平台时保护个人数据。注册和登录到学习平台需要学习者创建一个可靠的密码，保护密码和生物特征信息，以创造一个安全的在线学习环境。具体来说，在公共电脑上注册和登录时，应特别注意不要保存登录信息、不要在电脑屏幕上留下敏感信息、删除个人痕迹、禁用储存密码的功能等。

3) 浏览学习平台时保护个人隐私。对于参加 LMS 的课程，在线学习过程中利用个人学习服务，使用搜索引擎，识别本地服务，具体的解决方案和实践步骤都在这一部分进行了阐述，本节还讨论了如何备份重要数据。

4) 在使用社交网络工具学习时，确保个人资料的安全。在使用社交网络工具时，要注意合理利用网络研讨会，负责地在线讨论和在论坛发帖，安全上网等，针对这些问题的具体建议已经给出。

5) 在线学习结束后清理个人数据。在完成在线学习后，学习者需要做出是否删除数据的决定。本节讨论了如何删除数据和停用个人帐户的建议和方法。

由于在线学习或混合学习已成为一种流行的学习方式，这本书旨在提供在线学习期间保护个人数据的指导。以下五个问题值得我们重视。

1) 在线教育的价值应进一步得到关注。“确保包容性和公平的优质教育，促进人人享有终身学习机会”是教育 2030 可持续发展议程的目标。在线学习是实现这一教育目标的基础，它不仅适用于紧急时期的教育，也适用于未来教育。

2) 数据安全与个人隐私保护刻不容缓。在线学习过程中，个人数据保护的基本知识，如设置设备、注册在线学习平台、通过平台学习等，对个人数据安全具有重要意义。为了促进在线学习中个人隐私的保护，政府的政策标准、行业的技术保障体系以及其他利益相关者的行为应该携手为学习者营造一个安全的环境。

3) 在线学习是培养数字公民的重要途径。数字公民拥有有效利用信息技术与他人沟通、参与社会、创建与消费数字内容的知识和技能。在线学习已经成为学生学习的典型场景，在线学习的行为、习惯、观念等必然会影响他们的生活。引导学习者以适当的礼仪参与在线学习，可以培养有准备、有目的和有技能的数字公民。

4) 网络空间中的合作学习助力提升协同技能。个体通过彼此之间的互动和他们所生活的环境来创造意义。在线学习不仅仅是浏览内容，而是与内容、同伴、教师和环境进行互动。因此，学生可以利用工具和技术在网络空间与同伴和教师交流，同时了解如何在交流过程中保护自己的个人数据。

5) 融合数字学习与传统教学以支持弹性教学。学生可以自由选择时间和地点、数字资源、教学方法、学习活动和支持服务，这是未来的弹性学习模式。在线学习与传统学习的融合是弹性学习的前提。对这一融合的研究（包括融合过程中的个人数据保护）应该共享，以期为人类带来光明的未来。

参考文献

Aarhus University. (2020). Types of personal data. Retrieved from https://medarbejdere.au.dk/en/informationsecurity/data-protection/general-information/types-of-personal-data/

Acronis. (n.d.). Data Backup – What is it? Retrieved from https://www.acronis.com/en-us/articles/data-backup/

Amazon. (n.d.). Close Your Account. Retrieved from https://www.amazon.com/gp/help/customer/display.html?nodeId=GDK92DNLSGWTV6MP

Anderson, T. (2011). The theory and practice of online learning (2nd Edition). Edmonton, AB: AU Press.

Androws, T. (2019). How to Delete or Deactivate an Instagram Account [2020]. Retrieved from WaFtr: https://www.waftr.com/delete-instagram-account/

Apple. (n.d.). iPhone Theft and Loss Claims. Retrieved from https://support.apple.com/iphone/theft-loss-claims

Automatad. (2020). Consent Management Platform – Everything You Need to Know . Retrieved from: https://headerbidding.co/consent-management-platform-cmp

AWAKE. (n.d.). Network Intrusion. Retrieved from https://awakesecurity.com/glossary/network-intrusion/

AWAKE. (n.d.). Sophistication and Power Comes Built In. Retrieved from https://awakesecurity.com/product/

Baron, S. (2020). How to Back Up Data. Retrieved from wikiHow: https://www.wikihow.com/Back-Up-Data

Bloom, A., Attai, L .(2016). The ABCs of Student Data Privacy. America: McGraw-Hill Education.

Bodenham, L. (2017). How to manage your passwords safely. Retrieved from University of London: https://london.ac.uk/news-opinion/london-connection/top-tip/manage-passwords

Brotherton, C. (2017). Is Your Website GDPR Compliant? How to Get Ready for the General Data Protection Regulations. Retrieved from wpmudev: https://premium.wpmudev.org/blog/gdpr-compliance/

CANVAS. (2013). Day Five: Synchronous Learning Activities. Retrieved from https://learn.canvas.net/courses/45/pages/day-five-synchronous-learning-activities

ChildnetInternational. (2018). Staying safe online whilst livestreaming - advice for parents and carers. Retrieved from https://www.childnet.com/blog/staying-safe-online-whilst-livestreaming

Clarip. (2019). CCPA – Definition of Personal Information in California’ s Privacy Law. Retrieved from http://www.clarip.com/data-privacy/pi-definition-ccpa/

Committee of Ministers. (2010). the 1099th meeting of the Ministers’ Deputies. Retrieved from https://search.coe.

int/cm/Pages/result_details.aspx?ObjecctID=09000016805cdd00

Common Sense. (2018). How can teachers and students better protect their online privacy? Retrieved from https://www.commonsense.org/education/teaching-strategies/protect-your-students-data-and-privacy

Common Sense. (2018). How can teachers and students better protect their online privacy? Retrieved from https://www.commonsense.org/education/teaching-strategies/protect-your-students-data-and-privacy

CommonSpaces. (n.d.). Registration and authentication. Retrieved from https://www.commonspaces.eu/en/help/register/

Coursera . (n.d.). Delete your Coursera account. Retrieved from https://learner.coursera.help/hc/en-us/articles/209818563-Delete-your-Coursera-account

Coursera. (2019). how to delete my question? Retrieved from https://coursera.community/community-help-questions-40/how-to-delete-my-question-5289?postid=13141#post13141

Coursera. (n.d.). Leave your organization’ s learning program. Retrieved from https://learner.coursera.help/hc/en-us/articles/115001621606-Leave-your-organization-s-learning-program

CUCU, P. (2016). 17 Underused Online Shopping Security Tips. Retrieved from HEIMDAL SECURITY : https://heimdalsecurity.com/blog/online-shopping-security-tips/

Data Quality Campaign. (2015). What Is Student Data? Retrieved from https://dataqualitycampaign.org/resource/what-is-student-data/

Data Quality Campaign. (2016). Why Education Data? Retrieved from https://dataqualitycampaign.org/why-education-data/

Doneda, D. (n.d.). Privacy and Data Protection Frameworks in the 21st Century. An interview to Danilo Doneda. (UNESCO, Interviewer)

EcomSpark. (2019). How to deactivate or delete Facebook Account? Retrieved from https://www.ecomspark.com/how-to-deactivate-facebook-account/

Edmodo. (2016). Browse and Follow Communities (Teacher). Retrieved from https://support.edmodo.com/hc/en-us/articles/205009224-Browse-and-Follow-Communities-Teacher-

Edmodo. (2019). Delete a Post (Student). Retrieved from https://support.edmodo.com/hc/en-us/articles/205006664-Delete-a-Post-Student-

Edmodo. (2019). Delete a Post (Teacher). Retrieved from https://support.edmodo.com/hc/en-us/articles/205006474-Delete-a-Post-Teacher-

Edmodo. (2020). Deactivate a Student Account. Retrieved from https://support.edmodo.com/hc/en-us/articles/205011954-Deactivate-a-Student-Account

Edmodo. (n.d.). Communities and Topics. Retrieved from https://support.edmodo.com/hc/en-us/sec-

tions/200910674-Communities-and-Topics

ElectronicFrontierFoundation. (2006). Six Tips to Protect Your Search Privacy. Retrieved from https://www.eff.org/wp/six-tips-protect-your-search-privacy

Erika. M., Tim. G., Karen. S. (2010). Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). America: NIST.

EUROPEAN DATA PROTECTION SUPERVISOR. (2020). Rights of the Individual. Retrieved from https://edps.europa.eu/data-protection/our-work/subjects/rights-individual_en

FEDERAL TRADE COMMISSION. (2017). Children’ s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance

Flaherty, D. (1989). Protecting privacy in surveillance societies: The federal republic of Germany, Sweden, France, Canada, and the United States. Chapel Hill, U.S.: The University of North Carolina Press.

Francis, K. (2018). Major Goals And Expectations Of eLearning. Retrieved from elearningINDUSTRY: https://elearningindustry.com/goals-and-expectations-of-elearning-major

Gallagher, K., Magid, L., Pruitt, K. (n.d.). The Educator’ s Guide to Student Data Privacy. America.

Google. (2019). Helping kids be safe, confident explorers of the online world. Retrieved from https://beinternetawesome.withgoogle.com/en_us/

HestonKlare.（无日期）. 如何阻止网络霸凌 . 检索来源：https://zh.wikihow.com/ 阻止网络霸凌

Huang, R.H., Liu, D.J., Tlili, A., Yang, J.F., Wang, H.H., et al. (2020). Handbook on Facilitating FlexibleLearning During Educational Disruption: The Chinese Experience in Maintaining Undisrupted Learning in COVID-19 Outbreak. Beijing: Smart Learning Institute of Beijing Normal University.

HUCULAK, M. (2020). How to make a full backup of your Windows 10 PC. Retrieved from Windows Central: https://www.windowscentral.com/how-make-full-backup-windows-10

IAPP. (2017). Categories of Personal Data. Retrieved from https://iapp.org/resources/article/categories-of-personal-data/

IAPP. (2020). What does privacy mean? Retrieved from IAPP: https://iapp.org/about/what-is-privacy/

IDENTITYGUARD. (2017). How Your Old Phone Number is Putting You at Risk. Retrieved from https://www.identityguard.com/news/old-phone-number-putting-risk

IEEE. (2016). IEEE Announces Standards Project Addressing Data Privacy Processes and Methodologies. Retrieved from https://standards.ieee.org/news/2016/ieee_p7002.html

i-scoop. (n.d.). Data subject rights and personal information: data subject rights under the GDPR. Retrieved from https://www.i-scoop.eu/gdpr/gdpr-personal-data-identifiers-pseudonymous-information/

ISO . (2011). ISO/IEC 29100:2011(en) Information technology — Security techniques — Privacy framework. Retrieved from https://www.iso.org/standard/45123.html

IT Governance. (n.d.). The GDPR and Privacy Compliance Frameworks. Retrieved from https://www.itgovernance.co.uk/gdpr-privacy-compliance-framework-and-standards

Karnes, K. (2020). Push Notification Best Practices: 35 Tips for Dramatically Better Messages. Retrieved from CleverTap: https://clevertap.com/blog/push-notification-best-practices/

KNOWLEDGE@WHARTON. (2019). Your Data Is Shared and Sold…What’s Being Done About It? Retrieved from https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/

Knowliah. (2018). Categories of data in GDPR. Retrieved from https://www.knowliah.com/en/learn/categories-of-data-in-gdpr

Kowalski, P. (2017). If You Want Personalized Learning, Don’t Forget about Data. Retrieved from Data Quality Campaign: https://dataqualitycampaign.org/want-personalized-learning-dont-forget-data/

Lam, J. (2019). How to protect your personal data? Retrieved from lawinfographic: https://www.lawinfographic.com/protect-personal-data/

learning-styles-online. (n.d.). Overview of Learning Styles. Retrieved from https://www.learning-styles-online.com/overview/

Lloyd, J. (2020). How to Block Adult Sites. Retrieved from wikiHow: https://www.wikihow.com/Block-Adult-Sites#On-Windows-10

Maciej. Z., Michal. W. (2018). What Is a Consent-Management Platform (CMP) and How Does It Work? Retrieved from CLEARCODE: https://clearcode.cc/blog/consent-management-platform/

Martinelli, K. (2018). Password Security Guidance. Retrieved from High Speed Training: https://www.high-speedtraining.co.uk/hub/password-security-guidance/

MatuszewskaKarolina. (2020). Comparison of 5 Leading Consent Management Platforms. Retrieved from: PIWIK: https://piwik.pro/blog/consent-management-platforms-comparison/

Mikroyannidis, A. (2011). Supporting Self-Regulated Learning within a Personal Learning Environment:The OpenLearn case study. IEEE, (pp. 607-608).

Morin, A. (n.d.). Personalized Learning: What You Need to Know. Retrieved from Understood: https://www.understood.org/en/school-learning/partnering-with-childs-school/instructional-strategies/personalized-learning-what-you-need-to-know

Nield, D. (2019). How to switch phones without losing anything. Retrieved from PopularScience: https://www.popsci.com/switch-to-new-phone/

NIST. (2017). Standards and Guidance Cited in NIST Privacy Framework RFI Responses. America.

Norton. (n.d.). How safe is surfing on 4G vs. WiFi? Retrieved from: https://us.norton.com/internetsecurity-wifi-how-safe-is-surfing-on-4g-vs-wi-fi.html

NortonLifeLock. (n.d.). Dangers of Free Downloads. Retrieved from https://www.nortonsecurityonline.com/security-center/dangers-of-free-downloads.html

OECD. (2013). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Retrieved from https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

OFC. (2018). Protecting your privacy online. Retrieved from https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/protecting-your-privacy-online/

ORCID. (2019). Deactivating an ORCID account. Retrieved from https://support.orcid.org/hc/en-us/articles/360006973813-deactivating-an-orcid-account

Owyang, J. (2008). Understanding the difference between Forums, Blogs, and Social Networks. Retrieved from https://web-strategist.com/blog/2008/01/28/understanding-the-difference-between-forums-blogs-and-social-networks/

Panda. (2019). 8 Mobile Security Tips to Keep Your Device Safe. Retrieved from https://www.pandasecurity.com/mediacenter/panda-security/mobile-security-tips/

Pappas, C. (2016). eLearning Authoring Tool Costs: 7 Factors To Consider. Retrieved from elearningINDUSTRY: https://elearningindustry.com/elearning-authoring-tool-costs-7-factors-consider

PMaria. (2020). GDPR Privacy Policy Template. Retrieved from: PrivacyPolicies: https://www.privacypolicies.com/blog/gdpr-privacy-policy

Popescu, E., Ghita, D. (2013). Using Social Networking Services to Support Learning . Romania: Craiova University.

Privacy Technical Assistance Center. (2014). Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices . America.

PrivacyPolicies. (2020). Privacy Policies are Legally Required. Retrieved from https://www.privacypolicies.com/blog/privacy-policies-legally-required/#What_Is_A_Privacy_Policy

PrivacySense. (2016). Personal Information. Retrieved from http://www.privacysense.net/terms/personal-information/

ProtectingStudentPrivacy. (n.d.). What is an education record? Retrieved from https://studentprivacy.ed.gov/faq/what-education-record

邱丽芳 .（2019 年 9 月 5 日）. 谷歌和优兔将因儿童隐私问题支付 1.7 亿美元罚款 . 检索来源：新华网：http://www.xinhuanet.com/world/2019-09/05/c_1124965153.htm

ROBINSON, R. (2020). Data Privacy Vs. Data Protection. Retrieved from Ipswitch: https://blog.ipswitch.com/data-privacy-vs-data-protection

SafeOnline. (n.d.). How to Prevent Cell Phones From Being Tracked. Retrieved from https://safeonline.ng/communications/how-to-prevent-cell-phones-from-being-tracked/

SCORM. (n.d.). SCORM Explained 201: A deeper dive into SCORM. Retrieved from https://scorm.com/scorm-explained/?utm_source=google&utm_medium=natural_search

SecureControlsFramework. (2018). Secure Controls Framework (SCF) Privacy Management Principles.

SHAD, A. (2018). Top 10 Free GDPR Tools and Solutions You Didn’t Know Before. Retrieved from ECOMPLY.io: https://ecomply.io/top-10-free-gdpr-tools-and-solutions/

Student Data Principles. (n.d.). 10 Foundational Principles for Using and Safeguarding Students’ Personal Information. Retrieved from https://studentdataprinciples.org/the-principles/

STUDENTPRIVACYPLEDGE. (2015). K-12 School Service Provider Pledge to Safeguard Student Privacy. America.

TechTarget. (2007). hijacking. Retrieved from https://searchsecurity.techtarget.com/definition/hijacking

TEKETEIPURANGI. (2018). Choosing the right digital device. NewZealand.

The Western PA Healthcare News Team. (2017). Social Network Etiquette: How to Mind Your Manners Online. Retrieved from HealthcareNews: https://www.wphealthcarenews.com/social-network-etiquette-mind-manners-online/

Toledo, R. (n.d.). How to Protect Your Privacy on Your Mobile Devices. Retrieved from Lifehack: https://www.lifehack.org/articles/technology/how-protect-your-privacy-your-mobile-devices.html

Triella. (2018). WEAK PASSWORDS ARE STILL THE BIGGEST SECURITY RISK. Retrieved from https://www.triella.com/weak-passwords/

Wan, T. (2017). How to Protect Education Data When No Systems Are Secure. Retrieved from EdSurge: https://www.edsurge.com/news/2017-09-25-how-to-protect-education-data-when-no-systems-are-secure

Wikipedia. (2020). Information privacy law. Retrieved from https://en.wikipedia.org/wiki/Information_privacy_law

Wikipedia. (2020). Personal data. Retrieved from https://en.wikipedia.org/wiki/Personal_data

Wikipedia. (2020). Sharable Content Object Reference Model. Retrieved from https://en.wikipedia.org/wiki/Sharable_Content_Object_Reference_Model

WorldEconomicForum. (n.d.). Personal Data: The Emergence of a New Asset Class. Retrieved from https://www.weforum.org/reports/personal-data-emergence-new-asset-class

Zhan. T., Wang. X. (2020). Personal Data Security Technical Guide for Online Education Platforms. Russia: UNESCO Institute.

术语表

在线学习 (1.1)

在线学习指学生使用不同的设备（如移动电话、笔记本电脑等），在同步或异步环境中通过互联网进行学习的体验。在这些环境中，学生可以在任何地方自主学习，并能与教师和其他学生互动（Singh & Thurman，2019 年）。

个人信息 (2.1)

个人信息是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特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

—中华人民共和国民法典，第一千零三十四条

教育记录 (Education records) (2.2)

“教育记录”是与学生直接有关的记录，由教育机构或代表该机构行事的当事方保存。这些记录包括但不限于年级、成绩单、班级名单、学生课程时间表、健康记录 (K-12 年级)、学生财务资料 (高等教育程度) 和学生纪律档案。信息可以以任何方式记录，包括但不限于手写、印刷、计算机媒体、录像带、录音磁带、胶片、缩微胶卷、缩微胶片和电子邮件。

—34CFR99.2，美国家庭教育权利和隐私法（Family Educational Rights and Privacy Act of United States）

隐私 (2.2)

隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。

— 中华人民共和国民法典，第一千零三十二条

隐私政策 (2.3)

隐私政策是一种声明或法律文件 (隐私法)，它公开了一方收集、使用、披露和管理客户或客户数据的部分或全部方式。个人信息可以是任何可以用来识别个人的东西，不仅限于个人的姓名、地址、出生日期、婚姻状况、联系信息、身份证签发和到期日期、财务记录、信用信息、病史、旅行地点以及购买商品和服务的意图。

– McCormick, Michelle. “New Privacy Legislation.” Beyond Numbers 427 (2003): 10-. ProQuest. Web. 27 Oct. 2011

WiFi (3.2)

WiFi 是一种将电子设备连接到无线局域网 (WLAN) 的技术。WiFi 通常被称为无线网络。

虚拟专用网络 (VPN) (3.2)

虚拟专用网络 (VPN) 将专用网络扩展至公共网络，使用户能够通过共享网络或公共网络发送和接收数据，就好像他们的计算设备直接连接到专用网络一样。VPN 是通过使用专用电路或使用现有网络上的隧道协议建立虚拟的点对点连接而创建的。

安全套接字层协议 (SSL) (3.3)

SSL 是在 TCP/IP 协议之上实现的安全协议。SSL 支持各种网络，并提供三种基本安全服务，所有这些服务都是由一个公钥和一个对称密钥启用的。

统一资源定位符 (URL) (4.1)

统一资源定位符 (URL)，通俗地称为网址，是对网站资源的引用，它指定它在计算机网络上的位置和检索它的机制。

学习管理系统 (LMS) (5)

学习管理系统 (LMS) 是一种用于管理、记录、跟踪、报告、自动提供教育课程、培训项目或学习发展项目的软件应用程序。

> – Ellis, Ryann K. (2009), Field Guide to Learning Management, ASTD Learning Circuits, archived from the original on 24 August 2014, retrieved 5 July 2012

搜索引擎 (5.3)

搜索引擎通常是一个用来指网络搜索引擎的术语。网络搜索引擎或因特网搜索引擎是一个程序系统，用来进行网络搜索 (因特网搜索)，这意味着以系统的方式在万维网上搜索文本框中指定的特定搜索信息。 搜索结果通常显示在一行结果中，通常称为搜索引擎结果页 (SERPs)。

HTTP cookie (5.3)

HTTP cookie（也称为 Web cookie，Internet cookie，browser cookie 或简称 cookie）是从网站发送并在用户浏览时由用户的 Web 浏览器存储在用户计算机上的一小段数据。

位置服务 (LBS) (5.4)

基于位置的服务 (LBS) 是一个通用术语，表示利用地理位置数据和信息向用户提供服务或信息的软件服务。LBS 可以应用于多种场合，如健康、室内物体搜索、娱乐、工作、个人生活等。

社交网络和社交网络服务 (6)

社交网络是一种社会结构，由一组社会行为者 (如个人或组织)、一组二元关系以及行为者之间的其他社会互动组成。社交网络视角为分析整个社会实体的结构提供了一套方法，同时也提供了各种理论来解释这些结构中所观察到的模式。

社交网络服务 (也包括社交网站或社交媒体) 是一个在线平台，有着相似的个人或职业兴趣、活动、背景或现实生活中的联系的人们可以利用这个平台与其他人建立社交网络或社交关系。

> – Wasserman, Stanley; Faust, Katherine (1994).

域名系统 (DNS) (6.3)

域名系统 (Domain Name System, DNS) 是互联网的一项服务。它作为将域名和 IP 地址相互映射的一个分布式数据库，能够使人更方便地访问互联网。

主题索引

<table>
<tr><td rowspan="8">第三章
个人设备设置和学习工具选择</td><td rowspan="3">3.1
设置个人设备</td><td>级别
认识 / 警惕 / 保护自己 / 保护他人</td><td rowspan="2">主题
我可以选择哪些在线学习工具?</td></tr>
<tr><td>相关用户
学生、家长、老师</td></tr>
<tr><td>相关隐私
储存在设备内的个人数据，例如个人身份信息</td><td rowspan="2">主题
如何确保设备安全?</td></tr>
<tr><td>风险
· 遗失或被盗</td></tr>
<tr><td rowspan="3">3.2
管理网络连接</td><td>级别
认识 / 警惕 / 保护自己 / 保护他人</td><td rowspan="2">主题
如何将移动设备连接到互联网?</td></tr>
<tr><td>相关用户
学生、家长、老师

相关隐私
储存在设备内的个人数据，例如个人身份信息</td></tr>
<tr><td>风险
· 网络入侵
· 中间人攻击
· 浏览器劫持</td><td>主题
如何安全使用互联网?</td></tr>
<tr><td rowspan="3">3.3
选择和安装学习工具</td><td>级别
认识 / 警惕 / 保护自己 / 保护他人</td><td>主题
作为一名教师，我如何为学生选择工具?</td></tr>
<tr><td>相关用户
学生、家长、老师

相关隐私
个人身份信息，生物识别信息</td><td rowspan="2">主题
如何安全下载及安装软件?</td></tr>
<tr><td>风险
· 假冒或恶意网站
· 电脑病毒
· 恶意软件</td></tr>
</table>

第三章 个人设备设置和学习工具选择	**3.4** 浏览隐私政策	**级别** 认识 / 提高警觉	**主题** 如何找到隐私政策？
		相关用户 学生、家长、老师	
		相关隐私 基本资料	
		风险 · 在线学习工具滥用数据	
第四章 注册和登录时的隐私安全	**4.1** 创建账户的密码策略	**级别** 认识 / 提高警觉 / 保护自己	**主题** 如何设置强密码？
		相关用户 学生、家长、老师	**主题** 使用密码管理工具
		相关隐私 个人身份信息，网络身份信息	**主题** 如何使用谷歌浏览器或 iOS 生成强密码？
		风险 · 弱密码 · 密码泄露	**主题** 如何保护密码不会泄漏？
			主题 什么是生物识别标识？
			主题 如何保护我的生物特征信息？
	4.2 公共设备的安全问题	**级别** 认识 / 提高警觉 / 保护自己	**主题** 如何安全使用公用电脑？
		相关用户 学生、家长、老师	
		相关隐私 个人身份信息，网络身份信息	
		风险 · 用户信息泄露	

<table>
<tr><td rowspan="5">第五章
在线学习平台中的数据和隐私安全</td><td rowspan="3">5.1
课程注册与管理</td><td>级别
认识 / 提高警觉 / 保护自己</td><td>主题
如何报名参加课程？（例如 Coursera）</td></tr>
<tr><td>相关用户
学生、家长</td><td rowspan="3">主题
如何浏览和关注社区？（例如 Edmodo）</td></tr>
<tr><td>相关隐私
基本信息，出勤信息，首选内容，学习记录</td></tr>
<tr><td>风险
· 由于用户、站点或第三方造成的数据泄漏</td></tr>
<tr><td rowspan="4">5.2
个性化学习服务</td><td>级别
保护自己</td><td rowspan="4">主题
政策制定者和教育领导者在制定各种个性化学习策略时需要知道什么？</td></tr>
<tr><td>相关用户
学生</td></tr>
<tr><td>相关隐私
个人上网记录</td></tr>
<tr><td>风险
· 提取和恶意使用信息，如用户偏好和学习模式等
· 由于平台受到外部攻击而导致用户信息泄露
· 向第三方平台提供非法信息</td></tr>
<tr><td rowspan="4">5.3
使用搜索服务</td><td>级别
保护自己</td><td rowspan="2">主题
如何保护你的搜索隐私？</td></tr>
<tr><td>相关用户
学生</td></tr>
<tr><td>相关隐私
网络浏览痕迹</td><td rowspan="2">主题
如何屏蔽搜索引擎中的「cookies」？</td></tr>
<tr><td>风险
· 提取和恶意使用信息，如用户偏好和学习模式
· 由于平台受到外部攻击而导致用户信息泄露
· 向第三方平台提供非法信息</td></tr>
</table>

第五章 在线学习平台中的数据和隐私安全	**5.4** 管理定位服务	**级别** 认识 / 提高警觉 / 保护自己 **相关用户** 学生 **相关隐私** 个人位置资料 **风险** · 位置 / 信息泄露对人身和财产安全的威胁 · 由于平台受到外部攻击而导致用户信息泄露 · 向第三方平台提供非法信息	**主题** 如何防止手机被追踪?
	5.5 备份个人数据	**级别** 认识 / 提高警觉 / 保护自己 **相关用户** 学生，家长，老师 **相关隐私** 个人身份信息等 **风险** · 转售个人资料 · 广告 · 生命安全	**主题** 如何进行数据备份?
第六章 社交网络工具中的数据和隐私保护	**6.1** 使用视频会议工具	**级别** 认识 / 提高警觉 / 保护自己 **相关用户** 学生 **相关隐私** 个人位置资料 **风险** · 位置 / 信息泄露对人身和财产安全的威胁 · 由于平台受到外部攻击而导致用户信息泄露 · 向第三方平台提供非法信息	**主题** 在线直播时确保网络安全—给家长和监护人的建议

<table>
<tr><td rowspan="5">第六章
社交网络工具中的数据和隐私保护</td><td rowspan="4">6.2
发布网络信息内容</td><td>级别
认识 / 警惕 / 保护自己 / 保护他人</td><td>主题
社交网络中的基本注意事项</td></tr>
<tr><td>相关用户
学生、家长、老师</td><td rowspan="3">主题
注意网络礼仪</td></tr>
<tr><td>相关隐私
个人身份信息，个人财产信息，个人信息位置</td></tr>
<tr><td>风险
· 提取和恶意使用信息，例如用户用户偏好
· 由于平台受到外部攻击而导致用户信息泄露
· 向第三方平台提供非法信息</td></tr>
<tr><td rowspan="4">6.3
屏蔽不健康内容</td><td>级别
认识 / 提高警觉 / 保护自己</td><td>主题
如何屏蔽不适当的内容?</td></tr>
<tr><td>相关用户
学生</td><td>主题
如何管理你的推送通知?</td></tr>
<tr><td>相关隐私
个人上网记录</td><td rowspan="2">主题
应对网络欺凌</td></tr>
<tr><td>风险
· 提取和恶意使用信息，例如用户用户偏好
· 由于平台受到外部攻击而导致用户信息泄露
· 向第三方平台提供非法信息</td></tr>
<tr><td rowspan="5">第七章
个人信息删除</td><td rowspan="4">7.1
删除在线学习数据</td><td>级别
认识 / 提高警觉 / 保护自己</td><td rowspan="4">主题
如何删除用户生成内容?</td></tr>
<tr><td>相关用户
学生</td></tr>
<tr><td>相关隐私
个人身份信息，个人网络历史</td></tr>
<tr><td>风险
· 该平台不允许删除
· 删除后非法保留信息</td></tr>
<tr><td rowspan="4">7.2
注销账户</td><td>级别
认识 / 提高警觉 / 保护自己</td><td rowspan="4">主题
如何停用帐户?</td></tr>
<tr><td>相关用户
学生</td></tr>
<tr><td>相关隐私
个人身份信息，个人网络历史</td></tr>
<tr><td>风险
· 该平台不允许停用
· 禁用后非法保留信息</td></tr>
</table>

北京师范大学智慧学习研究院
Smart Learning Institute of Beijing Normal University

网 址： http://sli.bnu.edu.cn/en/
地 址： 北京市 海淀区
学院南路12号京师科技大厦A座12层

邮 箱： smartlearning@bnu.edu.cn
电 话： 8610-58807219
邮 编： 100082

HTTP://SLI.BNU.EDU.CN/EN/