许可使用政策(AUP)

阅读本行为准则时应结合《隐私声明》。

安全性

- 必须始终保护用于访问学校 IT 系统的用户名和密码的安全性。请勿与任何其他用户共享或尝试使用其他用户的密码。您将对使用您的用户名进行的任何系统操作负责。切勿向儿童提供登录的详细信息。
- 不允许在公众使用的任何设备上使用学校的访问凭证，例如酒店、图书馆或机场。也不允许为图便利而使用任何浏览器保存这些访问凭证——员工每次访问系统时都必须明确键入用户名和密码，而不是将这些信息记录在其他人可以发现的任何地方。应频繁更换密码以增加安全性。
- 您必须在使用完计算机或离开房间后进行注销。如果您暂时离开房间，请锁定计算机。
- 每天结束时应关闭计算机和任何白板投影仪或屏幕。
- 请勿尝试禁用或绕过学校的防病毒系统，在未经授权的情况下访问您无权使用的任何数据或系统，或损坏或破坏任何其他用户的数据或工作。

数据保护

- 请勿将机密信息或个人数据发送给无权阅读的人员。这样做将违反数据保护法规。
- 请勿从系统中复制个人信息或机密信息以供校外使用。
- 不得复制或打印儿童的行动计划。只能在学校网络上访问和更新行动计划。
- 切勿使用 USB 记忆棒，因为已不再提供这种数据移动方式，且这种方式也不可靠。
- 根据数据保护法规，记录的任何个人信息都可能是主题访问请求的主题，包括对个人的意见和意图。因此，请谨慎处理您记录和保存的数据。主题访问请求应首先提交给财务主管——切勿为回复该请求而发出个人数据。
- 确保任何个人数据始终处于全面安全的状态（计算机中的或纸张形式的个人数据）。
- 如果您认为可能发生数据外泄，则有责任立即通知财务主管。

电子邮件

- 只能使用学校的电子邮件系统发送和接收与学校有关的个人或机密电子邮件。**不得将学校电子邮件转发给不属于学校的个人电子邮件账户。**
- 在发送电子邮件之前检查其内容，确保收件人不会将其视为任何形式的骚扰或辱骂。
- 如果电子邮件中含有秘密发送给您的信息，请勿转发该邮件，也不得转发被指定者可能合理认为是机密信息的电子邮件。
- 不得将学校的电子邮件地址用于与学校工作无关的任何目的。
- 在必要的情况下将监控沟通的内容。因此，使用学校系统进行沟通的内容不能被视为是完全保密的。
- 监控的目的是确保学校系统主要用于促进学校工作，而不是用于不当和/或非法的目的，且该系统的容量足以满足学校的需求。
- 将对接收和发出的邮件进行过滤，以识别病毒和不可接受的附件，也可能针对不可接受的的语言进行过滤。在不警告发件人或收件人的情况下就可能拦截垃圾邮件。

图像

- 除非使用学校存储卡，否则不得在个人数码相机或移动设备上记录儿童的照片。如果您需要拍摄儿童的照片，您必须使用学校的一台相机和一个存储卡，并且只能将图像下载到学校的系统上。不得将儿童的图像下载到家用计算机上或将其上传到互联网，除非是上传到学校为此专门设计的系统。

在校外访问 IT 系统

- 在校外访问学校的系统/数据时应使用虚拟专用网络（VPN）。
- 使用 VPN 时，如果其他家庭成员共享安装了学校 VPN 软件的计算机，则应格外谨慎，以确保仅在员工使用计算机时才进行连接。用于任何学校工作的家用计算机必须用密码保护，并且该密码仅为相关工作人员所知。
- 如果您使用学校的笔记本电脑，IT 系统经理将记录您拥有该电脑的事实。您同意始终负责保管该笔记本电脑并保证其安全性。携带任何此类设备旅行时，必须将其作为手提行李且不得置于无人照管的状态。应尽可能对笔记本电脑进行加密。

软件

- 请勿下载任何可安装或可运行的软件，或将任何未经批准的软件安装到任何学校计算机上（即 Spotify、Dropbox 或类似软件）。请勿加载或运行游戏 CD、音乐 CD，或将任何 MP3 播放器、iPod、手机或类似设备连接到任何学校计算机上。

- 所有购买新软件的请求必须按照学校的采购政策处理
- 在提议使用新的软件供应商或新的应用程序时，请与人力资源和监察专员协商，以便与提议的供应商签订数据处理协议。
- 校方已获得软件所有者的许可协议，该许可协议对学校使用其软件作出授权。未经 IT 系统经理许可，不得在私人计算机上安装学校软件。这种做法极有可能侵犯版权或违反许可条款。

安全措施

- 必须采取所有合理步骤，确保儿童无法访问存储在网络上的机密数据和在无人监督的情况下访问互联网：
- 当您输入启动密码或登录密码时，请确保不会被儿童看到。
- 切记，过滤器可以减少但不能消除在互联网上暴露于不当材料的风险，理解这一点非常重要。负责监督的人员必须通过不断走动和与儿童讨论他们正在做的事来积极监督儿童。鼓励教师打开标签页并要求查看儿童的互联网访问历史。
- 确保教师在监督学生时知悉如何报告浏览到的不当文字和图片的正确程序。
- 您有责任尽最大努力确保儿童访问的内容与他们的年龄完全相适应，并确保儿童访问到与其年龄不相适应的内容时予以适当处理。
- 除非工作人员已阅读并完全理解《数字设备指南》（可从网站上提供），否则他们不得监督使用计算机的儿童。

网页浏览和社交媒体

- 学校使用系统来监控和过滤所有对互联网的访问/使用。该系统记录并限制对违禁站点（包含恐怖主义和极端主义材料）的访问，并使信息通信技术系统管理员能够立即向指定的安全措施主管报告问题。
- 请注意，访问某些不适当的网站可能构成刑事犯罪，并且网络过滤系统并非绝对可靠。
- 不得试图访问或下载儿童无法合理获取的材料。
- 在任何情况下，均不得故意访问、查看、存储、下载或转发任何非法、不当或任何冒犯性的材料（例如连锁邮件、色情内容和种族主义、性别歧视或其他歧视性的笑话等）。
- 请勿在网站、社交媒体、博客聊天系统或论坛等上发布与学校有关的评论、参考资料、信息或与学校或您在学校的工作有关的任何材料。
- 如果您无意中涉及不适当的材料，应立即通知指定的安全措施主管。

通过互联网与儿童联系

- 工作人员在任何时候均不得通过社交媒体与学生交换信息或文件，或通过互联网与儿童联系，因为这种做法可能会促进学生与工作人员控制范围之外的未知成年人之间产生其他联系。
- 工作人员不得与在校生发生微信、电子邮件或短信往来。
- 如果儿童提出任何其他问题，那么工作人员应提议按学校的正常安排与儿童面谈。
- 如果学生毕业离校但仍未满 18 岁，同样的规则将继续适用于社交网站，但简单、直接的电子邮件通信是可以接受的。但是，工作人员应当意识到对于所有年龄段的学生，电子通信都是一个潜在的危险领域，需要特别小心谨慎，以免涉及任何不适当的通信。
- 工作人员不得向家长或儿童透露个人电话号码。郊游时可能需要手机，但在这种情况下，应使用学校的手机。
- 工作人员不得在教室内使用手机，或将其用于直接与儿童接触的目的，不论是拨打电话、接听电话还是拍摄儿童照片。请参阅手机使用政策。

个人使用

- **学校的信息通信技术系统只能用于行使学校聘用您时要求您行使的职责。但是，允许有限地出于个人目的使用电子邮件和互联网设施。任何此类使用必须符合本政策，不得干扰员工履行职责或涉及访问过多的音频和视频材料。**
- 滥用或过度使用电话系统、电子邮件和/或互联网将通过处分程序予以处理。
- **学校无法支持、维护或以其他方式协助维护私人拥有的计算机设备。不得向学校的信息通信技术工作人员提及与个人计算机相关的问题，因为校方不允许他们从事此类工作，或未对此类工作投保。**唯一的例外是学校的 VPN 软件存在问题，而其故障是学校软件而不是个人的硬件或软件所导致的。
- 包括电话在内的学校信息通信技术设备不得用于赌博，也不得用于与学校无关的任何个人事务。
- **对于仅能通过互联网接入的银行或储蓄帐户，或其他金融、购物或交易帐户，如果学校网络为您提供的是接入此类账户的唯一途径，那么请勿开设此类账户。学校不能保证继续提供访问此类网站的权限，并且不能对遇到的任何困难负责。**

- 学校担心如果员工使用该网络存储个人文件，其系统上的空间可能会被不必要地消耗。必须仅限于储存学校使用的数码照片或数码视频。学校系统中的个人文件可能会被删除而不会发出警告或通知。

一般规则

- 不应将任何食物或液体带入任何使用信息技术的场所，因为这对儿童来说是一个坏榜样，同时存在溢出并在其后造成惊扰的风险。
- **集中监控打印行为。避免不必要的打印，并在适当的情况下考虑在纸张的双面打印并使用再生纸。除非绝对必要，否则请勿进行彩色打印。请勿将学校的打印设备用于个人用途。**

网络使用政策

协议

通过以下签名，您确认已阅读并接受《网络使用政策》中所述的使用圣约翰学院南京分园 IT 系统的行为准则。

您同意从签名之日起即受该内容的约束，无论您是否在该日期开始参与学校工作。

姓名 _____

签名 _____ 日期 _____