上海静安区四季在线培训学校
信息数据交互及处理能力和个人信息保护制度

为了保障学校网络用户的合法权益，保护用户的隐私信息，依据《中华人民共和国网络安全法》等法律法规，参考国家标准 GB/T 35273—2017《信息安全技术 个人信息安全规范》，制定本制度，以加强对用户个人信息的数据采集、存储、使用等个人信息处理活动的监管。

一、 数据分级

1. 本规范所称数据是指，由用户产生的或因用户所处环境、个人设备等产生的所有数据。由公司自发产生的相关数据（例如人事数据、财务数据、战略规划等）不属于本规范约定的数据范围。
2. 公司对数据实行分级管理。
3. 根据用户数据的敏感程度的高低，将用户个人数据分为：隐私数据、重要数据、公开数据三个级别。
4. 隐私数据定义：能够单独或者与其他信息结合识别自然人个人身份及特征的数据。隐私数据一旦泄露、非法提供或滥用可能危害人身和财产安全，可能导致个人名誉、身心健康受到损害或歧视性待遇等损害后果。主要有以下几种类型：

隐私数据	隐私数据举例
个人健康生理信息类	如：身高、体重、医疗记录等
个人生物识别信息类	如：指纹、声纹、虹膜信息、面部信息等
个人身份信息类	如：身份证（号）、护照（号）、社保卡（号）、居住证（号）等
个人财产信息类	如：银行账号/卡号、信贷记录、存款信息、交易记录等
个人轨迹信息类	如：用户精确地理位置、行踪轨迹、住宿信息等
个人通信信息类	如：聊天记录、通话记录、通讯录、短信记录、好友列表、群聊列表等

个人基本信息类	如：真实姓名、生日、邮件地址、联系地址、用户名、手机/座机号等
个人身份认证信息类	如：系统中的账号、邮箱地址、密码、访问令牌、密保答案、用户证书等
个人教育工作信息类	如：职位、工作单位、学习经历、工作经历、培训记录、成绩单等
以及安全部门认定属于隐私数据的其他数据类型。 特别说明：14 岁以下（含）儿童的个人信息为隐私数据。详细规定参见上课端“儿童隐私政策”之相关规定。 https://share.eeo.cn/s/agreement/?type=child_privacy&lang=zh-CN	

5. 重要数据定义：不能够单独或者仅凭这些数据，定位、识别、显式标记自然人个人身份的数据，主要有以下几种类型：

重要数据分类	重要数据举例
个人基本资料类	如：民族、宗教信仰、国籍等
网络身份标识信息类	如：昵称、IP 地址、个人签名栏等
个人学习记录类	如：如报名课程、测验结果、学习时长、学习偏好等
个人上网记录类	如：访问日志、操作日志、排错记录等
个人设备信息类	如：硬件序列号、设备 MAC 地址、软件列表、击键记录、IMEI、IMSI 等
以及安全部门认定属于重要数据的其他数据类型	

6. 公开的个人数据、不属于个人隐私数据和重要数据的其他数据类型，认定为公开数据。

二、 采集规范

1. 对数据的采集应当以公司名义、通过公司的渠道进行，不得以员工个人名义向用户索取或者收集相关数据。
2. 对于数据的采集，应当遵循最少需要原则，不得采集超过业务需要的数据。

3. 隐私政策和用户授权
    1) 如果应用程序或站点试图收集数据，则必须以法律法规要求的方式向用户提示隐私政策，或显式征得用户授权。
    2) 用户拒绝接受隐私政策或拒绝授权收集信息的，在不收集数据的基础上还能向用户继续提供服务的，可以继续提供服务，否则应当中止当前服务。
    3) 隐私政策以集团法务提供的内容为准。
4. 数据上报
    1) 数据上报的接口必须强制 HTTPS。
    2) 数据内容必须经过加密，且加密所需密钥长度不低于 64Bits。
    3) 原则上禁止向集团外的第三方系统上报数据。
5. 数据采集方法
    1) 禁止采用动态下发可执行文件/程序的方式执行数据采集。
    2) 数据采集的 SDK 应当进行强度足够的混淆和加壳处理。
6. 隐私数据采集
    1) 原则上，除非业务需求无法避免，否则禁止采集隐私数据。
    2) 隐私数据的采集应当由集团相关部门审批，必要时需集团 COO 审批，集团横向统一组织实施。
    3) 对隐私数据的采集应当显式地征得用户同意，用户未显式同意的，应当认定为用户拒绝授权收集。
    4) 用户拒绝收集隐私数据的，不得收集。
7. 重要数据采集
    1) 对于重要数据的采集，原则上应当交由数据分析部门或集团统一组织实施。
    2) 在采集重要数据之前，应当征求用户许可，用户不许可的，不得收集。
8. 数据去标识化
    1) 数据去标识化是指通过对数据的技术处理，使得主体无法被识别，且处理后的数据不能被复原的过程。

2) 经过去标识化的信息可以在不征得用户显式同意的情况下商业化利用。

3) 原则上，对于内部需要公开使用的数据应当进行数据去标识化处理。

三、 存储规范

1. 将采集到的数据以任何方式保存下来称为数据存储。
2. 除非业务必需，隐私数据应当加密存储。
3. 鼓励对重要数据的加密存储。
4. 加密存储数据的，应当采用加密强度足够的算法和密钥。
5. 原则上，隐私数据的存储应当由集团统一组织实施，重要数据的存储应当由数据分析部门或集团统一组织实施。
6. 对于存储隐私数据或重要数据的计算机或服务器，应当由运维部门或数据库管理部门统一安排维护。
7. 除服务器运维人员外，其他人员不得拥有存储隐私数据或重要数据的计算机或服务器管理权限。
8. 采集隐私数据或重要数据时，在用户端禁止明文落地存储。
9. 对于业务确实需要且经过集团审批的，方可在业务线存储隐私数据或重要数据，但需要继续遵守本规范规定的相关义务，承担相关的责任。

四、 使用规范

1. 所有使用隐私数据和重要数据的人员或业务系统均需遵守本章规定。
2. 无合理的业务需求时，不得使用隐私数据和重要数据。
3. 不鼓励使用者使用数据时直接接触数据。
4. 原则上禁止导出隐私数据或重要数据，确实因业务需求，需要导出相关数据的，还应当遵守《数据导出管理规范》。
5. 如需要对数据进行分析，原则上应以需求的方式交由数据分析部门完成，以报表的形式交付结果。
6. 数据分析部门可以依据本规范，结合具体业务状况，制定进一步实施细

则。

7. 对于隐私数据，原则上禁止交由第三方使用，但法律法规规定提供的除外。
8. 对于隐私数据和重要数据，确因业务需要提供给第三方使用的，应当通过集团相关部门审批，必要时需经集团 COO 审批，并与第三方签署保密协议。

五、 访问审计

1. 运维部门或其他数据管理部门，应当记录数据的访问日志，以供审计。
2. 访问日志至少包括: Who（访问者）、When（发生时间）、What（访问了什么数据）、Why（访问数据的原因）。
3. 访问或使用相关数据的人员、业务系统均应当接受审计，审计应当公正、客观。
4. 审计工作由集团安全部门、法务部门、人力资源部门或内审部门组织或联合组织进行。
5. 在审计过程中发现有证据证明存在异常访问数据的，应当依照本规范奖惩条款 9.1 处理。

六、 监督

1. 集团安全部门将依据本规范，对数据采集、存储、使用的情况进行检查。
2. 检查的结果将上报集团相关管理层。

七、 奖惩

1. 未经授权使用、披露隐私数据或重要数据的，将上报人力资源部，追究相关人员责任。
2. 因违反公司规章制度造成数据泄露的，将上报人力资源部，追究相关人员的责任，违反中国法律法规造成数据泄露的，将追究相关人员的法律责任。

3. 在审计过程中弄虚作假的，将上报人力资源部，追究相关人员责任。

八、 规范负责人

上海静安区四季在线培训学校技术中心信息安全部负责本规范的解释。

上海静安区四季在线培训学校

2021 年 11 月 1 日