

防灾科技学院

钉钉移动协同工作平台安全权限设置说明

一、组织机构

1. 人事处负责维护二级机构及三级机构名称（以学校文件为依据）；
2. 部分部门（安全处、后勤处、图书馆）可以自行维护四级及以下机构，其他部门无维护权限；
3. 所有人员可查看组织机构；
4. “校领导”仅办公室可看。

二、通讯录

1. 正常运行期间，人事处负责维护二级机构及三级机构中人员的入职、岗位变更、离职，维护人员信息变更；
2. 部分部门（安全处、后勤处、图书馆）可以维护四级及以下机构人员信息的变更；
3. 通讯录基本信息在组织机构范围内全部开放，每人每天最多可查看通讯录信息 5 个；
4. 通讯录显示的基本信息有部门、姓名、手机号、职位、邮箱、办公地点、办公电话；
5. 员工人事信息字段仅人事处、组织部可见；
6. 部署实施期间，人事处提供全体在岗工作人员信息，员工加入平台的审批工作暂由信息化管理中心负责，实施完

成后的正常运行期间，由人事处指定专人负责加入审批和日常人事管理；

7. 全体在岗工作人员在使用移动协同工作平台时应遵守各项法律法规，禁止将学校组织架构、通讯录发布到移动协同工作平台以外；注重保护个人隐私，慎重对“钉钉”开放个人手机联系人访问权限。

三、工作台

1. 本次部署实施期间，物业报事保修单、审批、电话会议、视频会议、钉邮、钉盘功能面向全体人员开放；

2. 智能人事功能面向校领导、人事处开放；（测试完成后面向全校开放）

3. 智能会议室功能面向校领导、办公室开放；（测试完成后面向全校开放）

4. 平台公告由办公室和宣传部共同维护；读取权限面向全校开放；

5. 阿里商旅面向校领导、财务处开放；（测试完成后面向全校开放）。

四、消息

1. 学校全员群仅二级机构主要负责人以上人员发言，其他人员禁言；

2. 部门群组以及其他自由组建的工作群组由群主承担管理责任；

3. 在使用移动协同工作平台时应遵守各项法律法规，在群组沟通中禁止发布与工作无关的信息，禁止将对话消息、群组发言发布到移动协同工作平台以外。

五、“钉钉”移动协同工作平台的安全概况

1. 符合国际、国内认证：钉钉通过 ISO27001 国际认证以及国家公安部三级认证，这是国际和国内最高等级的认证，证明钉钉已经符合了国际及国内的安全认证标准；

2. 双重加密：钉钉采用双层加密模式，在信息传递过程中钉钉和第三方双重加密，这保证无论是钉钉还是第三方，没有一方是能独立获取用户数据的；通过第三方加密的信息，即使是公安部门要求钉钉提供数据，也必须到相应的公司获取密钥，钉钉无法破解客户的加密信息；

3. 技术保障：钉钉背靠阿里强大的技术资源，阿里神盾局拥有 10 多年的网络安全攻防经验，多达 1000 名安全技术工程师为钉钉提供了金融级别的技术保障（跟支付宝的安全级别一致）。而且钉钉的数据采用分布式存储，有效避免了数据被攻击后可能出现的外泄和丢失。与此同时，阿里巴巴对于信息安全的管控机制十分完善，密钥和数据分团队管理，同时获取密钥和数据的难度极高；最后，钉钉的数据不与任何部门或公司共享，钉钉绝对不搞大数据，充分保障企业的数据仅归属于企业自己；

4. 钉钉开放平台上的所有第三方应用都入驻了钉钉云

服务永续计划和无忧保障计划,由钉钉来保障应用的数据安全和服务稳定;

5. 客户群体: 在钉钉的客户体系中,浙江省人民政府已经全面使用钉钉,并且社区和村一级也已经全部覆盖;G20 峰会的指挥中心、杭州市公安局、浙江大学、复星集团、红蜻蜓、链家地产、海底捞也都在用钉钉。