

# 保密宣传月 | 守住不能说的秘密！



## 关于保密知识，你知道多少？

### 一、什么是国家秘密？

国家秘密是关系国家的安全和利益，依照法定程序确定，在一定时间内只限一定范围的人员知悉的事项。

### 二、国家秘密等级如何划分？

国家秘密的等级分为“绝密”“机密”“秘密”三级。

★“绝密”：是最重要的国家秘密，泄露会使国家的安全和利益遭受特别严重的损害。绝密级不超过 30 年。

★“机密”：是重要的国家秘密，泄露会使国家的安全和利益遭受到严重损害。机密级不超过 20 年。

★“秘密”：是一般的国家秘密，泄露会使国家的安全和利益遭受损害。秘密级不超过 10 年

### 三、国家秘密的基本范围有哪些？

《保密法》规定，国家秘密包括下列秘密事项：

- (1) 国家事务的重大决策中的秘密事项。
- (2) 国防建设和武装力量活动中的秘密事项。
- (3) 外交和外事活动中的秘密事项以及对外承担保密义务的事项。
- (4) 国民经济和社会发展中的秘密事项。
- (5) 科学技术中的秘密事项。
- (6) 维护国家安全活动和追查刑事犯罪中的秘密事项。
- (7) 其他经国家保密工作部门确定应当保守的国家秘密事项。
- (8) 政党的秘密事项中，符合国家秘密诸要素的，属于国家秘密。



### 四、保密载体有哪些？

涉密载体，是指以文字、数据、符号、图形、图像、声音等方式记载国家秘密信息的纸介质、光介质、电磁介质等各类物品。

### 五、复制保密载体有哪些方面需要注意？

- (1) 复制本机关、本单位产生的机密级、秘密级涉密载体，应当经主管领导批准；复制其他机关、单位产生的涉密载体，应当经制发机关、单位批准，未经批准不得复制。
- (2) 复制涉密载体不得改变其密级、保密期限或删除国家秘密标志。

(3) 复制涉密载体应当履行登记手续，加盖复制机关、单位的戳记。复制件要采取与原件相同的保密措施。

(4) 复制涉密载体应尽量在本机关、本单位内部进行，需要送外单位复制的，应当委托具有涉密载体印刷资质的单位复制。

(5) 严禁复制绝密级涉密载体。确因工作需要复制的，属于本机关、本单位产生的，必须经本机关、本单位主要领导批准；非本机关、本单位产生的，须经原密级确定机关、单位或者其上级机关批准。



## 六、打电话、发短信也会造成泄密事件吗？

普通电话存在串音和载波辐射问题，有的电话线是暴露在外的，可以被搭线窃听，如果在通话中谈论国家秘密，就会造成泄密。而手机通信传输系统，是开放的无线通信系统，通信信号是在空中传输的，只要有相应技术设备，就可以截听通话内容。同时，手机还可以与互联网无线连接，所以在手机通话中谈论涉密内容或用手机发送或存储涉密信息，很容易造成涉密。

## 七、保密法对国家秘密信息的管理方面有哪些禁止性规定？

- (1) 禁止非法复制、积累、存储国家秘密；
- (2) 禁止在互联网及其他公共信息网络或者未采取保密措施的有线和无线通信中传递国家秘密；
- (3) 禁止在私人交往和通信中涉及国家秘密。

## 八、为什么不能在互联网及其他公共信息或者未采取保密措施的有线和无线通信中传递国家秘密？

互联网、固定电话网、移动通信网、广播电视网等公共信息网络，以及没有保密措施的有线和无线通信，都无法确保传递的安全，不能用来传递国家秘密，应当使用有相应等级保密措施的有线和无线通信设施、设备。

#### 九、工作人员保密行为十不准要牢记

1. 不准将工作中所知悉秘密泄露给无关人员
2. 不准将涉密计算机或存储介质接入互联网
3. 不准用非涉密计算机传真机处置涉密信息
4. 不准在移动电话普通电话中谈及涉密事项
5. 不准私自复制留存遗弃或向他人出借密件
6. 不准携带密件回家或在家中处理涉密信息
7. 不准携带密件探亲访友或至工作无关场所
8. 不准私自将密件带出境外或参加涉外活动
9. 不准在著述或个人邮件等公开信息中涉密
10. 不准擅自接受媒体采访或者发布涉密信息



# 保密宣传教育月 | 警惕微信泄密，做好保密工作！



保密工作，是党和国家历来高度重视的一项事关最高利益的重要工作。保守国家秘密，也是每位公民应尽的义务。随着互联网技术的高速发展，移动通信工具走入大众视野，它们成为了人们生活和工作中的好帮手。对于机关单位而言，好帮手有时却成了泄密的工具。近年来，微信泄密问题屡禁不止、高发频发，成为了名副其实的泄密“重灾区”。本期内容以微信为代表，谈谈移动通信工具如何从好帮手变为泄密“利器”，以及我们应该如何做好保密工作。

## 微信泄密案例：

### 案例 1

#### “文件传输助手” 导文件

#### 为图方便留隐患

2020年9月保密检查发现，某部属单位干部马某使用的非涉密计算机违规存储3份机密级文件。经查，原来是马某为方便起草材料，擅自将涉案文件拍照并制成PDF文档

后，通过微信“文件传输助手”导入涉案计算机使用，材料起草完成后，又立即删除了手机和计算机桌面上的文件文档。马某自认为“神不知鬼不觉”，但殊不知该文档已被微信电脑客户端自动备份到文件夹中。案件发生后，马某被给予党纪政务处分。

文件传输助手作为手机和电脑间图片文件等传输的有利便捷工具，却在不知不觉间存留了机密内容在网上存在流转的证据。



## 案例 2

### “朋友圈”发布文件首页

### 炫耀身份惹祸端

2019年7月，某市直属机关新任干部蒋某按照工作安排，到市委参加有关会议并领取1份秘密级文件。为炫耀公务员身份，蒋某将该文件首页拍照并在微信“朋友圈”发布。10分钟后，蒋某的领导孙某看见后立即责令其清除照片，但为时已晚，蒋某朋友金某已保存该照片并将其发布到个人微博，造成泄密。案件发生后，蒋某被给予党纪政务处分。

朋友圈本是人们分享日常生活的平台与窗口，如果反将其作为炫耀展示优越性的舞台，机密内容遭到泄密并极有可能在网上被大肆传播进而影响相关工作运转与社会治理。



### 案例 3

## 工作群众中交办工作

### 泄密只在顷刻中

2020年5月，某县教体局从机要渠道收到省委有关专项工作组下发的1份秘密级文件后，该局局长批示传达至各学校落实，办公室借调人员胡某为尽快落实文件精神，将文件全文拍照并发布至各学校校长微信工作群。某校校长张某未经查看即将文件照片转发至该校教师工作群，文件立即被群成员多次转发，迅速在数十个微信群传播，造成泄密。案件发生后，胡某、张某均被给予党纪政务处分。

微信群的存在为有相同工作任务的人员提供了沟通与交流相关事宜的平台，以增强联动性、协调性与便捷性。可是机密文件不加制约规范在不同微信群间的传播便造成了机密的泄密。



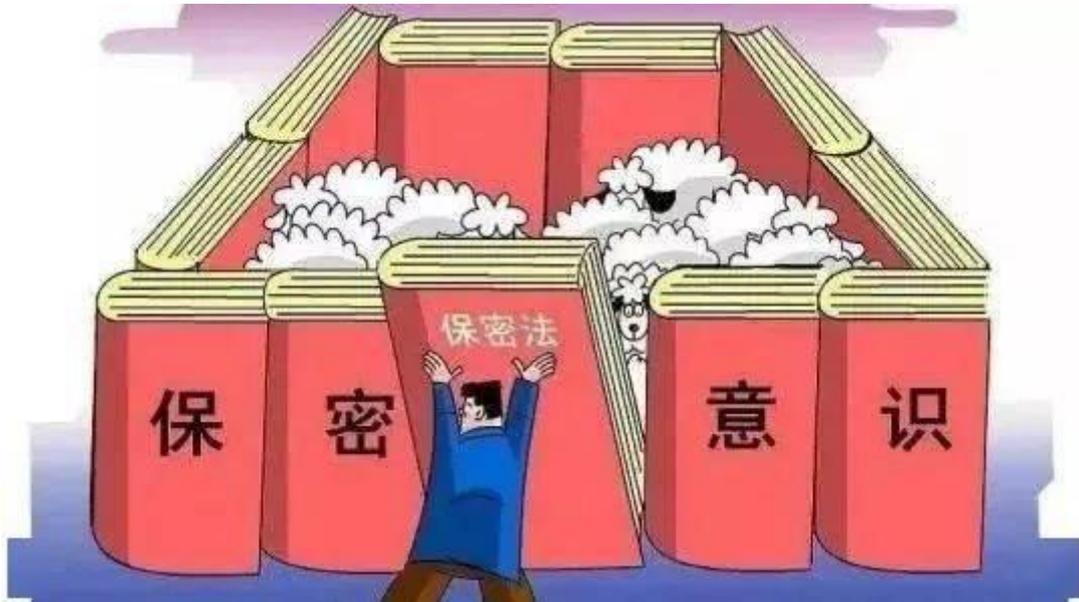
#### 案例 4

### “点对点”传递涉密文件

### 盲目轻信酿苦果

2019年3月，某县公安局辅警武某被选入该县某热点案件专案组协助工作，兴奋之余，在微信聊天时向好友程某称其掌握该案实际情况。在程某的再三打听下，武某将该案件汇报材料的主要内容拍照后发给程某，并嘱咐程某切勿外传。程某收到后，为显示自己有公安机关“人脉”，又转发给朋友肖某，同样嘱咐肖某勿传给他人。但案件当事人系肖某亲戚，肖某立即向其透露了公安机关办案情况。案件发生后，武某被司法机关依法追究刑事责任。

# 这七种心理，最易导致微信泄密



## “鸵鸟”心理

有的同志认为，微信传发信息多如牛毛，有关部门的涉密信息管理肯定不能面面俱到，即使能够全面覆盖，也不过是用关键词简单搜索，只要使用拼音、字母、别字、谐音等方式作一下模糊处理，或者拍成图片、使用语音、转换格式传发，就可以神不知鬼不觉地躲避。这种心理，恰似遇到威胁就把头埋进沙子的鸵鸟，实属掩耳盗铃、自欺欺人。在近年来的微信泄密案件中，不乏当事人采取自作聪明的规避措施，有的甚至采取对方阅看之后迅速“撤回”的招数，但都造成了严重后果。

## 捷径心理

有的同志只求工作效率，不顾保密纪律，在传达上级精神和领导指示时，觉得使用微信一键发送、静待回复的做法省时省力。这种心理，究其根本是把保密纪律当成了工作开展的“绊脚石”，而非保护国家安全利益和个人前途命运的“安全绳”，表面上便捷了工作，实则方便了敌特窃密。2020年，某单位干部李某通过微信群传达1份秘密级通知，案件发生后被处行政记过处分。李某在接受调查时坦言，其单位在外人员有10多个，手头上事情一多就想走“捷径”，忽视了保密纪律，现在想来悔不当初。

## 炫耀心理

有的同志不以保密为责任、却把知密当“本事”，工作中知晓了外界关注的涉密信息，迫不及待地想在微信群“爆料”、在朋友圈发帖，明目张胆地把涉密信息“炫耀”出去。这种心理，本质上是虚荣心作祟。为了成为朋友眼中的“消息灵通人士”“圈里人”，不惜把关乎国家安全利益的秘密信息当成提升个人影响力的资本。2017年，某领域改革方案初步确定，某单位干部强某看到后觉得涉及圈内好友的切身利益，就私自拍摄方案草稿，通过微信向好友通风报信，被好友发至其单位微信群，引起疯狂转发和热烈讨论，给改革大局造成严重干扰。



## 自恕心理

有的同志在遇到传达紧急事项或者上级催要材料时，觉得当务之急是想方设法抓紧完成任务，选择便捷的微信联系没什么问题，只要自己的出发点是为了工作，即使违反了保密纪律也无伤大雅、情有可原。这种心理，本质上是没认清一旦发生泄密问题意味着工作归零的道理，以致本末倒置、是非颠倒。2019年，某单位干部廖某使用微信传达1份机密级的紧急通知，在接受调查时非但没有悔意，反而觉得自己很冤枉，称“时间那么紧，不用微信根本传达不过来”，直到面对调查人员“为什么不发动骨干分头传达”“是泄密危害大还是传达延误危害大”的质问，才幡然醒悟、后悔不迭。

## 从众心理

有的同志看到别人使用微信传发涉密信息，觉得即使违规了，追究起来也是法不责众，如果在这样的“小事”上也规规矩矩，会被别人看成胆小怕事。最终，自己也成为“破窗效应”的俘虏，盲目跟风违反保密纪律。这种心理，本质上是在常见的违规现象面前丧失了独立思考，动摇了本就不够牢固的保密意识，被裹挟着“集体闯红灯”。2021年，某单位干部游某值班期间收到1份秘密级通知，想起单位平时用于交流的微信群里常有人发送内部信息，便盲目效仿，拍照上传。案件发生后游某对调查组说：“以前也学习过微信泄密的通报，但总觉得身边人这样发了都没事，就没把通报当回事。”

## 无知心理

有的同志“身在密中不知密”，认为有些秘密信息没什么敏感性，发到微信上也无妨；有的同志认为，微信本身采用了先进的安全保密技术，只要点对点传发信息，就不会泄密；还有的同志认为，自己只是把信息发给同事，不会扩散到“不可收拾”的地步。事实上，互联网向来是情报搜集的重要来源，开放的互联网社交平台更是各国情报机构监测的重点，信息一经发布就像断了线的风筝，一传十、十传百，传播范围完全不可控。2021年，某单位工作人员冯某看到1份新出台的涉密政策文件后，通过微信拍照发给同事时某，并再三交代“别往外传”。而时某并未遵守诺言，转而将文件照片发给其他人，最终传播链不断延长、全面失控，冯某、时某均被严肃处理。



## 旁观心理

有的同志遵循“事不关己、高高挂起”的人生哲学，看到微信群、微信朋友圈传发涉密信息，觉得若要好心提醒会被当作多管闲事，向组织报告会被当作“背后捅刀子”，只要自己默默“潜水”“围观”，追责就找不到自己头上，至于泄不泄密与己无关。这种心理，本质上是不愿得罪人的“老好人”思想，实际上既没有履行公民保密义务，又助长了乱发

乱传的不良风气。2020年，某单位干部吕某在单位微信群中传发涉密信息后，先后被3个微信群转发，而这3个群中近百名同事，竟没有一人出面提醒制止，默视涉密信息全面扩散。最终，3个微信群管理员都被追究相应责任。

欲治顽疾，先除心魔。遏制微信泄密问题多发频发势头，要求我们每个人必须从自身做起，心存戒惧，严守底线，共同维护国家秘密安全。

# 保密宣传教育月 | 这些保密问题要注意



近年来，基层干部职工保密违法案件高发频发，对国家安全和利益造成损害。相关单位、个人亟须加强对保密工作的认识，提升失泄密防范能力，筑牢安全保密防线。

典型案例基层干部职工保密违法行为常见于以下几种类型：

## 涉密计算机违规外联

2018年11月，有关部门在工作中发现，某县直单位1台涉密计算机发生违规外联。经查，A省审计组赴该单位开展工作时，要求其提供1台互联网计算机，该单位网络管理员张某遂根据领导安排，将某长期在外借调人员所用的计算机提供给审计组使用。在未核实该计算机是否涉密的情况下，张某将该计算机连接互联网并更改IP地址，触发违规外联报警。案件发生后，张某及有关责任人员均被依法给予相应的处理。



### **非涉密计算机违规存储、处理涉密文件。**

2021年7月，有关部门发现某县直机关工作人员江某使用的非涉密计算机中存储了3份涉密文件。经查，两年前江某在起草材料时，需要参考、引用上述涉密文件内容，为免去打字“麻烦”，便以光盘刻录的方式将之导入到个人使用的非涉密计算机中，直至被发现。案件发生后，江某被依法给予政务处分。



### **手机拍摄、微信传输涉密文件。**

2021年10月，有关部门发现某市属单位微信工作群传递1份秘密级文件。经查，该单位工作人员赵某根据领导钱某安排，在未履行审批手续的情况下，将该文件复印多份，并由钱某将之交给党务工作干部孙某，要求孙某尽快组织大家学习，孙某立即将文件全文

拍照并上传至党支部微信群，造成泄密。案件发生后，赵某、钱某、孙某均被依法给予政务处分。



### **门户网站发布涉密信息。**

2021年11月，有关部门发现某市属单位门户网站发布1篇会议消息稿，其中涉及1份机密级文件的主要内容。经查，该会议系该单位对上述涉密文件专题学习动员会议，严格按照涉密会议管理要求召开。但会议结束后，工作人员唐某在起草消息稿时，自认为已脱密处理，未履行定密程序便送办公室主任李某进行信息公开保密审查，李某也未认真审核，随意签发，导致该稿件流出，造成泄密。案件发生后，唐某、李某均被依法给予政务处分。分析建议以上案例不仅反映出个别干部职工保密“两识”的欠缺，更暴露了相关单位保密管理的短板。只有真正把保密责任扛在肩上、落实在行动中，从制度建设、宣教培训、监督检查等多方面发力，才能真正守牢基层保密防线。

# 保密宣传教育月 | 汇编文件严管理



汇编文件资料，是机关、单位非常普遍的一项工作。

这项工作一般耗时较长、任务繁杂、工作量大，在源头采集、编辑处理和保存使用等环节，稍不注意就容易出现失泄密问题。

## 案例 1：

2013 年，有关部门在工作中发现，A 省某县政府网站刊登了 1 份秘密级文件。经查，2010 年 11 月，县委组织部工作人员刘某为编制《干部业务手册》（以下简称《手册》），通过互联网搜索，从网上下载了 1 份与此相关的秘密级文件（未标密），未经核实便编入《手册》。2012 年 6 月，刘某又从《手册》中选出了包括涉案文件在内的部分政策法规文件，未经保密审查，便交由县政府网站负责人李某上传至网站，导致泄密。案件发生后，有关部门给予刘某行政警告处分，对李某进行警示提醒谈话。

本案中，刘某将从互联网上搜索到的文件未经认真核实便编入《手册》，且不经保密审查便上传至网站，导致泄密



## 案例 2

闫某系某政法大学刑事侦查专业硕士研究生，研究方向为物证技术。2015年9月至2016年3月，为撰写硕士论文收集资料，闫某从学校图书馆借阅了《刑事科技导论》《XX市公安局2010—2013年刑事案件汇编》等书籍资料，部分标注“秘密”或“内部资料 严禁外传”，又从其所属的刑事司法学院资料室借阅了《2009年XX省公安机关政内保典型案例》《刑事勘验与现场绘图指南》等书刊，其中有1份标注“机密”。经查，闫某都办理了普通的借阅手续，学校图书馆虽制定了关于涉密书刊资料外借和复制的规章制度，但没有得到严格执行，学院资料室仅在固定资产管理规定中提及涉密资料应当专人管理，但没有真正落实。闫某对借阅书刊资料进行拍照（部分使用文字识别软件转换为电子文档），保存在个人笔记本电脑中，在向其导师、校外导师报送稿件以及向7家杂志社投递稿件时，使用互联网邮箱传递了1份涉密资料。核查中还发现，闫某有使用互联网云盘备份资料的习惯，在其云盘上存储了大量专业资料，部分属于公安机关警务工作秘密信息。事件发生后，学校上级主管部门组织对互联网上的涉密及内部信息进行清理，该政法大学重新制定了涉密书刊资料使用管理细则并指定各级管理责任人，同时给予闫某记过处分，对其作出硕士论文内审不合格及延期毕业处理。

汇编文件资料涉及国家秘密的，应当按照规定报批，不得擅自改变原件的密级、保密期限和知悉范围；在汇编过程中，要和原文件认真、反复比对，确认密级、标题、文号、发文单位及年份等，避免漏看、漏审，出现弄错文件、忘记标注密级或者密级高低误标等情况。汇编本形成后，要按照汇编文件的最高密级和最长保密期限，在汇编本封面标注国家秘密标志，每本汇编本还要打印编号。

此外，涉密文件资料汇编本涉及的密件较多，务必要严格管理。汇编本在使用时，要按照其中文件资料所限定的最小知悉范围使用，不得擅自扩大知悉范围。机关、单位对于汇编本的使用情况要随时跟踪掌握，要按照汇编本的编号逐一登记发放，确保一旦出现问题有据可查。



# 保密宣传月 | 高校承担涉密科研项目要 谨防泄密



高校不仅担负着高层次人才培养的重任，也承担了大量的涉密科研项目。由于高校具有科研氛围宽松、日常管理灵活、人员流动性大等特点，在涉密科研项目保密管理方面往往存在一定的薄弱环节。个别高校师生保密意识淡薄、知识技能欠缺，违规操作时有发生，导致保密违法案件频发，甚至造成泄密后果。

## 典型案例

2021年6月，某高校申报承担了一项秘密级科研项目。6月29日，项目参与者——该校教师李某、莫某，将该秘密级项目任务书送委托方办理相关手续。在此期间，由于李某另有任务提前返回学校，由莫某独自办理。莫某在委托方单位附近一家无涉密载体印制资质的复印店将任务书复印3份，一份交委托方，另两份连同原件带回后，交与项目参与者——该校教师汤某。7月2日，项目参与者——该校教师陶某在互联网计算机上填写了项目有关审查表，标注为秘密级，将审查表拷贝至汤某个人U盘。7月6日上午，汤某让学生梁某用手机应用软件扫描任务书转入互联网计算机，并拷贝至汤某个人U盘。之后，汤某

将 U 盘中存储的涉密任务书、审查表拷贝至个人互联网计算机中，合并成一个文档，使用电脑版微信转发给莫某修改。调查中发现，汤某与莫某两人多次互传该文档。7 月 8 日，汤某又将该文档转发至项目组微信群，造成泄密。案件发生后，汤某、莫某被给予纪律处分，陶某、梁某以及其他负有监管责任、领导责任的人员均受到相应处理。



在上述泄密案件中，涉及多种常见的保密违法行为：

**保密违法行为一：**违规私自复制涉密文件。莫某明知有关项目任务书属于国家秘密，擅自在路边复印店使用非涉密复印机复印，违反了复制涉密文件应当按照规定报批的要求。

**保密违法行为二：**使用手机软件扫描、处理涉密文件。

**保密违法行为三：**在互联网计算机中存储、处理涉密文件。保密法第四十八条将使用非涉密计算机、非涉密存储设备存储、处理国家秘密信息作为违反保密法行为之一。

**保密违法行为四：**使用微信传递涉密文件。



团结奋斗新征程  
保守秘密靠大家



010-55601919  
发现泄密问题，请拨打电话

国家保密局 宣