Working with KPMG

—

Let's do this

Working with KPMG– v.3

We do what is right: Integrity at KPMG - 2023

Global Code of Conduct

Our Values

Speak up

Ethical Decision Making framework – CARE
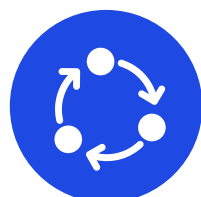
CEAC

Engagement performance

Bribery

Confidential information

Insider trading

Independence

Reporting requirements

← **Click each icon to learn more.**

Links to the KPMG policies will be available only for third parties with a KPMG account.

Our ethical and collaborative culture

At KPMG, our ethical and collaborative culture is critical to achieving our trust and growth ambition, and our long-term success as a business.

✓ It helps us attract and retain the best people and be the kind of workplace that **you** want to work in.

✓ It provides a foundation for our relationships with our clients, the entities that we audit, regulators, strategic alliance partners and vendors and other stakeholders.

✓ It underpins the trust that our clients, our people, our stakeholders, and society at large have in us. This trust is essential if we are to accelerate our growth and capture additional market share.

Our commitment to upholding our Values is clear: there is **never** a situation – either inside or outside of our work at KPMG – where compromising our standards of behavior is acceptable.

Our ethical and collaborative culture grows stronger when we all take personal responsibility for living our Values in everything that we do and we hold each other accountable for doing so.

The Global Code of Conduct

The Global Code of Conduct (the Code) guides our actions both inside and outside of KPMG. It includes:

Our Values	Our Commitments	Our Responsibilities	Where to get help	Compliance with the Code of Conduct

The Code expressly sets out the ethical behaviors expected of everyone at KPMG. It defines what it means to work at and be part of KPMG, as well as our individual and collective responsibilities.

See the following for more details:

- Global Code of Conduct
- 5.6.1 Comply with Laws, Regulations and Professional Standards

Our Values: What we believe

Integrity

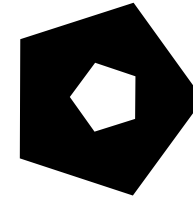We do what is right.

Excellence

We never stop learning and improving.

Courage

We think and act boldly.

Together

We respect each other and draw strength from our differences.

ForBetter

We do what matters.

Click each value to learn more

More information on our Values including a short introductory video can be found on the Values Portal

Integrity

We do what is right.

What it means

- Consistently leading by example with high standards and morals

- Being honest and truthful in words and actions

- Navigating pressures honestly, in a challenging environment

Integrity means we are honest, fair and **consistent** in our words, actions and decisions — both inside and outside work. We take **responsibility and accountability** for our day-to-day behavior and we hold ourselves to the **highest moral and ethical standards** at all times — even when **under pressure**. We keep our promises and set an example for others to follow.

Key themes

Honesty, fairness, keeping promises, accountability

Excellence

We never stop learning and improving.

What it means

- Setting the standard for and executing with quality

- Continuously building on current performance and culture

- Taking responsibility and accountability for actions

Excellence means relentlessly **delivering quality work to the highest professional standards.** We do this by staying **curious and taking personal responsibility for our learning.** We constantly look to improve our work through **data and insight**, and are **open to new challenges and feedback** because that is how we develop and improve.

Key themes

Quality, professional standards, going beyond, continuous learning

Courage

We think and act boldly.

What it means

- Communicating openly and directly

- Striving for innovation and new thinking

- Relentlessly pursuing differentiation in the market

Courage is about being **open to new ideas** and **being honest** about the limits of our own knowledge and experience. It's about **applying professional skepticism** to what we see and **asking questions where we have doubts.** We **speak up** if we see something we believe is wrong and we **support those who have the courage to speak up themselves.**

Courage is being **bold enough** to step outside of your comfort zone, to do what is right and meaningful for all stakeholders.

Key themes

Speak up, feedback, innovation, confidence

Together

Click here to go back to the Our Values overview

We respect each other and draw strength from our differences.

What it means

- Showing care and consideration for others

- Embracing diversity and acting inclusively

- Collaborating within and across teams

We do our **best work when we do it together**: in teams, across teams, and by working with others outside our organization. Working together is important because we know it's **collaboration that shapes opinions** and drives creativity. We embrace people with **diverse** backgrounds, skills, perspectives and life experiences and ensure different voices are heard. We show **care and consideration** for others and strive to create an **inclusive environment** where everyone feels they belong.

Key themes

Collaboration, inclusion, care, belonging

For Better

We do what matters.

What it means

- Serving and strengthening our markets and communities

- Making the firm better for future generations

- Making a positive impact on society

For better means taking a **long-term view**, even in our day-to-day choices, because we want to build a **stronger KPMG for future.** We never lose sight of the importance of our role in **building trust** in the capital markets and in business. We make **sustainable, positive change** in our local communities and in society at large, **striving to make the world a better place.**

Key themes

Long-term view, stewardship, society, purpose

Speak Up

⟨ ⟩

You're required to report potential or suspected violations of KPMG policy or applicable laws, regulations or professional standards. This includes situations when you know or suspect that colleagues, clients or parties associated with clients, or suppliers, subcontractors or associated third parties are engaged – or may be about to engage – in illegal or unethical activity. At KPMG, you can speak up and raise issues without fear of retaliation – we have zero tolerance for **any** form of retaliation, and appropriate action will be taken to address the matter.

See 5.6.2 Report Non-compliance by Clients or Third Parties, 5.6.3 Report Breaches of KPMG Policy by a KPMG Member Firm or Personnel and 14.2.6 Process to Report Suspected Non-compliance with Laws and Regulations or with KPMG Policies for details.

KPMG offers many channels of communication to seek guidance and raise concerns. You should never feel you're alone when faced with an ethical dilemma.

Resources closest to the situation (e.g. an engagement partner) may be in the best position to resolve an issue. Depending on the issue, you may want to consider other channels. Always choose the channel you feel most comfortable with. The important thing is that you speak up!

| Supervisor, line manager, or performance manager | Engagement partner | Ethics and Independence Partner (EIP) | Risk Management Partner (RMP) | KPMG International Hotline (KPMGI Hotline) | Other reporting channels outside your member firm |

Speak Up

Engagement manager/KPMG contact person

Contact manager or KPMG contact person to discuss issues or concerns you are facing. You can also report misconduct that can be addressed or appropriately escalated.

Engagement partner

Contact your engagement partner for matters that relate to his or her clients, including: (1) non-compliance with laws or regulations by clients or third parties, and (2) breaches of KPMG policy or non-compliance with laws, regulations or professional standards by KPMG firms or personnel.

Ethics and Independence Partner (EIP)

Contact your EIP in the case of breaches relating to ethics and independence matters by KPMG firms or personnel.

Independence breaches should be reported immediately.

Risk Management Partner (RMP)

Contact your RMP on matters not involving clients (as you would usually report client-related matters to the engagement partner). If you believe the engagement partner is in some way involved in the matter or is not dealing with an issue in the appropriate way, escalate the matter to your RMP.

Speak Up

‹ ›

KPMG International Hotline (KPMGI Hotline)

The KPMGI Hotline is available, and you may find it useful if you feel uncomfortable or have concerns about using a channel of communication within your KPMG firm.
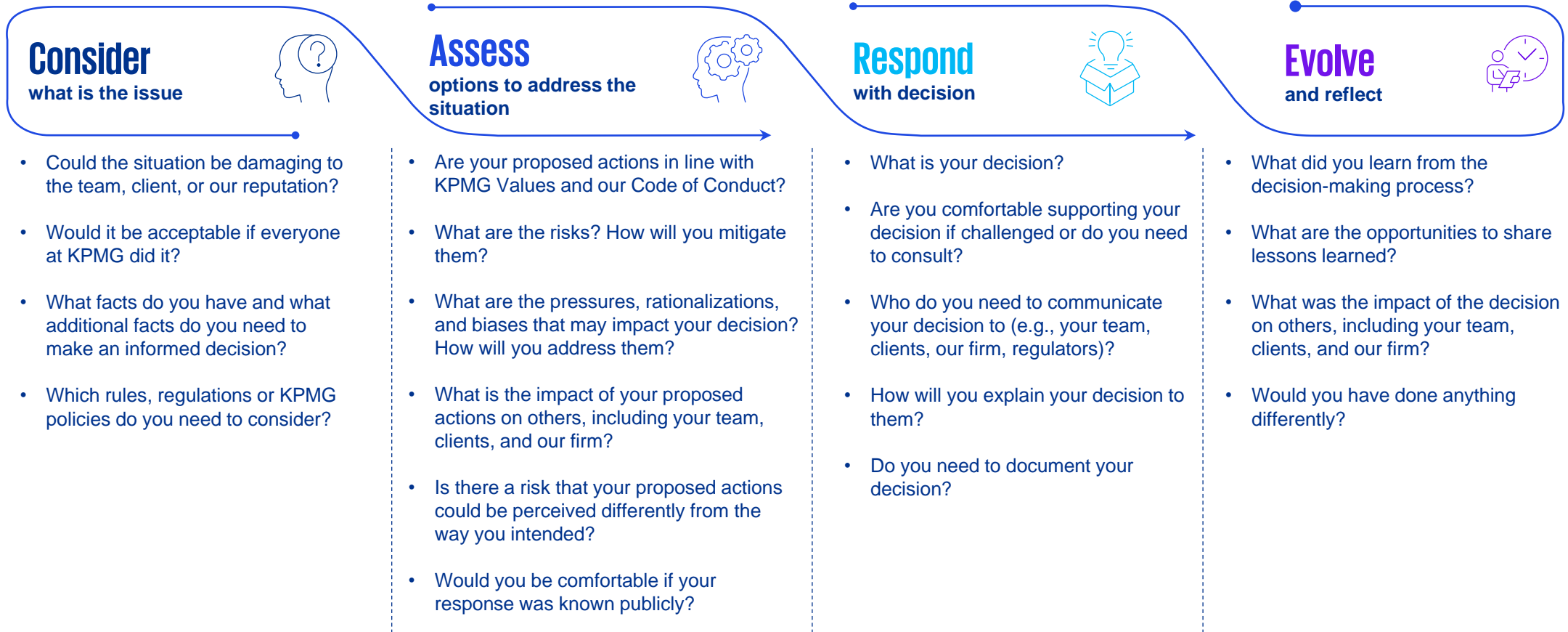
The KPMGI Hotline is managed by KPMG International personnel and provides confidential, anonymous reporting.

Other reporting channels outside your member firm

In addition to the individuals who support the KPMGI Hotline, here are some other individuals from outside your KPMG firm to consider contacting:

- Global Quality & Risk Management
- International Office of General Counsel
- Your Regional Risk Management Partner

Ethical decision-making framework – CARE

Consider
what is the issue

- Could the situation be damaging to the team, client, or our reputation?

- Would it be acceptable if everyone at KPMG did it?

- What facts do you have and what additional facts do you need to make an informed decision?

- Which rules, regulations or KPMG policies do you need to consider?

Assess
options to address the situation

- Are your proposed actions in line with KPMG Values and our Code of Conduct?

- What are the risks? How will you mitigate them?

- What are the pressures, rationalizations, and biases that may impact your decision? How will you address them?

- What is the impact of your proposed actions on others, including your team, clients, and our firm?

- Is there a risk that your proposed actions could be perceived differently from the way you intended?

- Would you be comfortable if your response was known publicly?

Respond
with decision

- What is your decision?

- Are you comfortable supporting your decision if challenged or do you need to consult?

- Who do you need to communicate your decision to (e.g., your team, clients, our firm, regulators)?

- How will you explain your decision to them?

- Do you need to document your decision?

Evolve
and reflect

- What did you learn from the decision-making process?

- What are the opportunities to share lessons learned?

- What was the impact of the decision on others, including your team, clients, and our firm?

- Would you have done anything differently?

Consult and Communicate – at any point

CEAC

<>

Who we work with and the work we do matters

It is important that we each understand we have a shared responsibility under the Code of Conduct and our Impact Plan to ensure the client and engagement decisions we make are aligned with our business strategies, Our Values and ethical principles.

Our risk management policies and our client and engagement acceptance continuance (CEAC) processes help us navigate those decisions to reach the right conclusions.

Working together to ensure we are completing the CEAC processes and carefully considering our client and engagement decisions, we will sustain and grow our brand in the global market and achieve our Trust and Growth ambition.

If you have questions or concerns arising from client and/or engagement acceptance and continuance decisions that may not align with our Values, it is your responsibility to speak up through one of the many Channels of Communication that are available.

Engagement performance

‹ ›

Upholding our Values of Integrity, Excellence, Courage, Together, and For Better will allow you to serve our clients and the public interest with pride.

Here are some considerations when working on engagements.

Be alert

Follow-up

Exercise professional skepticism

Documentation

Avoid bias

Click on the boxes to learn more.

Engagement performance

< >

Be alert

If something looks questionable or you suspect that something may be wrong, be skeptical – don't believe everything you're told. Keep asking questions until you're satisfied the issue has been appropriately addressed.

Potential issues concerning client personnel or others within your member firm should be reported immediately to your engagement partner or RMP.

Engagement performance

Follow-up

Always follow up on potential issues. Ensure that all matters are appropriately assessed, and any reporting requirements are met.

Engagement performance

Exercise professional skepticism

Never simply accept the client's version of events!

Examples of client situations that you should raise questions about include:

- The use of agents to make payments in high-risk environments or industries such as natural resources, construction, defense, and pharmaceuticals or jurisdictions with a high risk of corruption.

- Requiring KPMG to use certain third parties, such as a particular sub-contractor, for the engagement.

- Recent dismissal of its current auditors within a month of its filing deadline.

- Awarding of substantial commercial contracts (such as a construction contract for a new building or the awarding of a major government contract in a jurisdiction with a high risk of corruption) without open (or any) competition.

- The business model and operations are unclear, involve holding companies and special purpose vehicles located in known tax havens

- Inability to provide support for large regular payments to a third party.

Obtain appropriate evidence to support the evaluation of and the conclusions reached by you and your engagement team on these events.

Engagement performance

Documentation

The working papers must document the issue(s) you've found, the evidence obtained, and the issues' resolution, so that there are no 'loose ends.'

Consider whether your internal legal counsel should be involved in reviewing and finalizing the working papers.

Engagement performance

Avoid bias

Be careful not to be biased in your evaluation of matters and in decision-making. Do not make the mistake of assuming that the client or the people you know could never be involved in bribery, corruption, any other illegal or unethical act, or any other activity that may be damaging to the KPMG brand.

Bribery

⟨ ⟩

KPMG has zero tolerance for bribery and corruption in any form by anyone at KPMG and by those we may have dealings with. We are committed to conducting business fairly and ethically, and avoiding even the perception that KPMG or its people would offer or accept a bribe to obtain an advantage.

Be careful that offering or receiving gifts and entertainment doesn't cast doubt on KPMG's or your own integrity, independence, objectivity or judgment.

See the following policies for more details:

- 5.7.1 – Prohibition Against Involvement in Bribery
- 5.7.2 – Facilitation Payments
- 5.7.3 – Inducements including Gifts and Entertainment and consult your KPMG firm's gifts and entertainment policy for further guidance on local requirements including limits
- 14.4.1 – Appropriate Anti-bribery Steps in Relation to Supplier Organizations
- 14.4.2 – Internal Controls in Connection with Bribery
- 14.4.4 – Restrictions on Political Donations
- 14.4.6 - Member firm Anti Bribery and Corruption assessment exercise
- Які ми? - KPMG Ukraine KPMG Ukraine anti-bribery programe
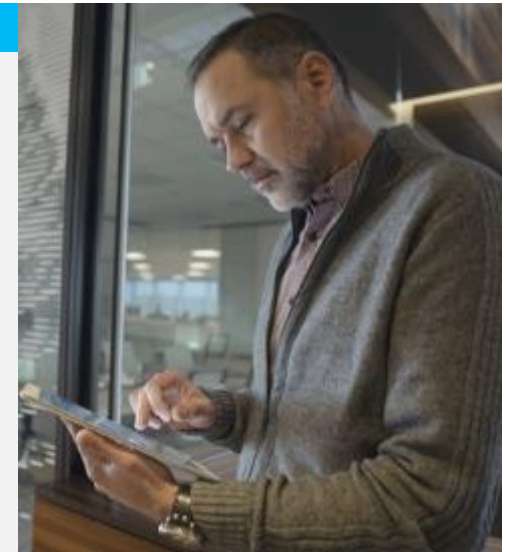
Confidential information

Most of the information that KPMG creates, collects and shares is sensitive in some way and everyone has an essential part to play when it comes to protecting it.

Under no circumstances should you use it confidential or sensitive information to your own advantage or the advantage of others. Do not disclose it outside of KPMG or share it with someone internally who doesn't have a business need to know it.

Follow KPMG policies and procedures to protect confidential information anywhere and everywhere you work including when you are working from home. You may think the risk of a confidentiality breach is lower when working from home, but the risk is actually increased and extra care should be taken to maintain confidentiality when working from remote locations, including home.

Many jurisdictions have specific laws and regulations on confidentiality as well as data privacy. Know and comply with the laws and regulations that apply to you and the work that you do.

! If you believe that confidential information and/or equipment used to store such information has been lost, stolen or otherwise compromised, immediately report the matter following your KPMG firm's procedures.
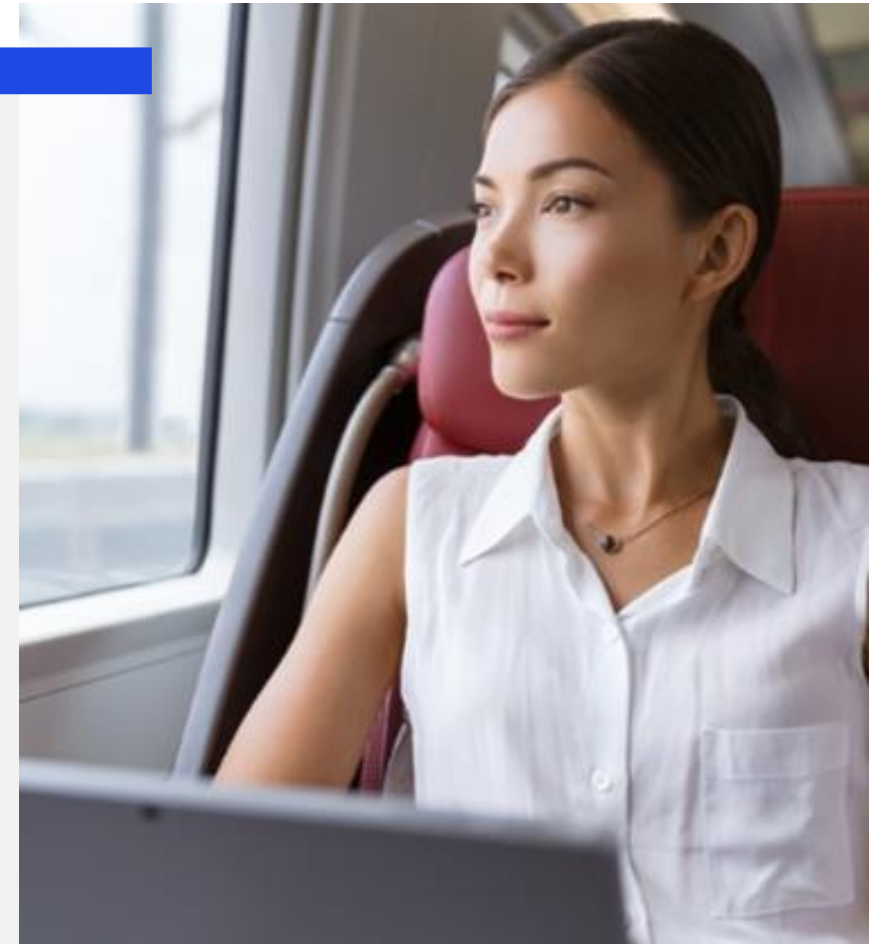
🔗 See 5.3. Confidentiality and Personal Information for details.

Protecting confidential information

‹ ›

No matter where you work – at home, at your KPMG office or workspace, or at a client location – here are some tips to keep confidential information and your KPMG technology resources safe and secure. *See also KPMG's Global Acceptable Use Policies for more details.*

- Confidential information must only be stored in a KPMG-approved technology solution.

- Lock or secure portable devices, including laptops, phones and USB drives at all times – including when you are traveling.

- Use a laptop security screen and lock your laptop screen when leaving your desk temporarily.

- Never share your password or other credentials with anyone.

- Collect and use only the information you need. Return or properly dispose of it as soon as it's not needed (subject to our retention policies).

- Never leave confidential papers, etc. unattended on your desk, at a printer or anywhere else.

Protecting confidential information

‹ ›

No matter where you work – at home, at your KPMG office or workspace, or at a client location – here are some tips to keep confidential information and your KPMG technology resources safe and secure. *See also KPMG's Global Acceptable Use Policies for more details.*

- Use only KPMG-approved, secure and encrypted storage devices and KPMG-approved software and apps.

- When sending emails, especially group emails, ask yourself: "Do they all really need to know this?"

- Be careful and select the correct persons when adding addressees to an email.

- Think before opening attachments or clicking on links in emails.

- Take care with conversations in public places, at home and when traveling.

- Use a meeting room or other private space when having a confidential conversation by phone, Skype or Microsoft Teams.
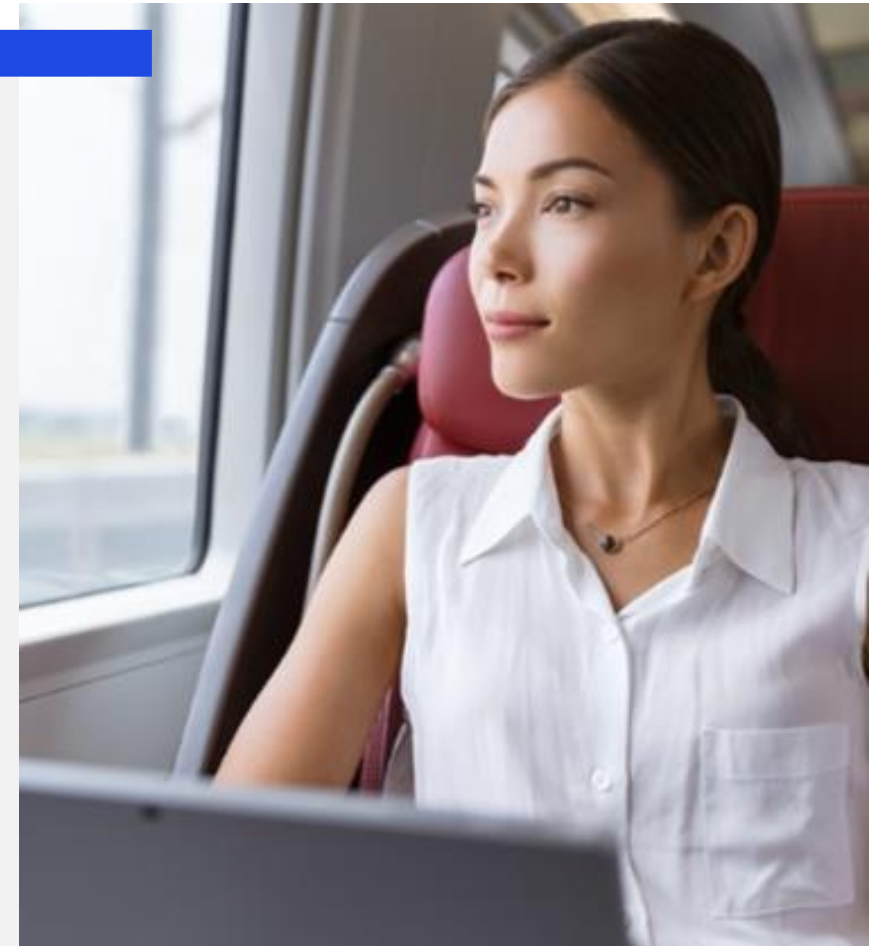
Insider trading

When you work at KPMG, irrespective of your role, you may become aware of non-public information relating to a given company or its securities. This is called **inside information**.

Trading of a public company's stock or other securities based on material, non-public information is known as insider trading.

Engaging in insider trading is against KPMG policy. Many countries have specific laws prohibiting insider trading, and other countries may have more general criminal and/or civil laws that are used to penalize this type of behavior.

Any KPMG person found to have violated KPMG's policy on insider trading will be subject to disciplinary action up to and including separation of partnership/employment. Any KPMG person in violation of insider trading laws may also be subject to criminal prosecution.

🔗 See 5.6.5 Insider Trading for details.

Independence

Independence is made up of two parts: independence of mind and independence in appearance:

> Being independent of mind means interests and relationships with our audit and assurance clients do not threaten our integrity, objectivity and professional skepticism in the conduct of our work.

> Being independent in appearance means that our integrity, objectivity and professional skepticism do not seem questionable to someone outside of the situation.

Independence issues can be complicated, so KPMG has provided a number of resources to help you navigate situation where you may not be able to determine what steps to take to comply with laws, regulations and firm policies that apply to you.
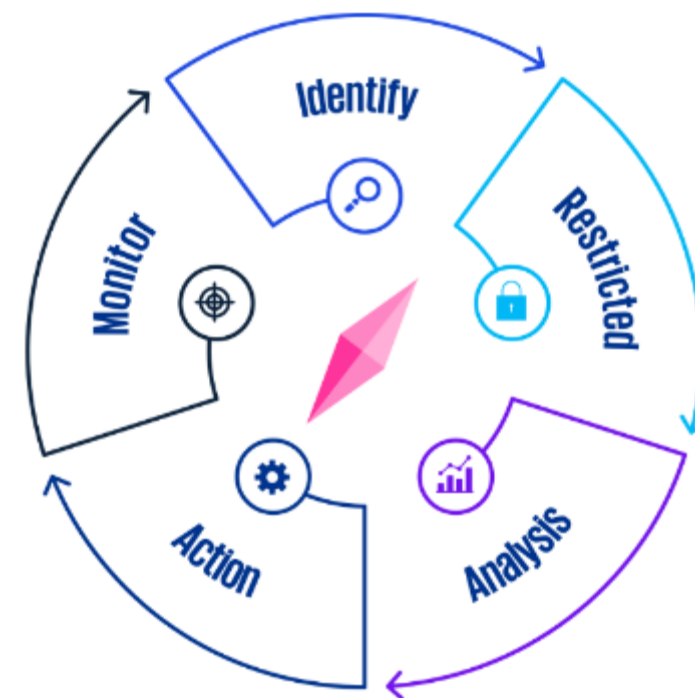
! You may be familiar with Independence Awareness Cycle tool. [Click here](#) for a refresher.

Reporting requirements – non-compliance with laws and regulations

⟨ ⟩

Within KPMG we have long-standing requirements in the Global Quality & Risk Management Manual to report potentially illegal acts. The IESBA Code of Ethics also includes provisions about non-compliance with laws and regulations by clients (and third parties acting under their direction) that affect all personnel, not just those in Audit.

This applies to all laws and regulations, not just those you may expect to encounter in a professional context.

- If you come across any situation where you think a client or third party has failed or may have failed to comply with a law or regulation, you need to notify the engagement partner.

- The engagement partner in turn, depending upon the facts and circumstances, is required to report the matter to others.

Click on the boxes below to learn more.

Non-compliance by clients or third parties

Process to report

What does this mean for you?

Non-compliance by clients or third parties

< >

Policy 5.6.2 Report Non-compliance by Clients or Third Parties covers requirements for KPMG personnel to report suspected or identified matters of non-compliance with laws or regulations.

It also includes additional requirements for an engagement partner to report certain matters to the RMP.

Be aware that you, as well as KPMG, may be required under applicable law or regulation to report suspicions of non-compliance with laws or regulations in a particular way to a particular person.

Process to report

Under Policy 14.2.6 Process to report suspected non-compliance with laws and regulations or with KPMG policies, your member firm is required to establish and maintain a process to report suspected non-compliance with laws, regulations, KPMG policies or professional standards by clients, third parties or KPMG personnel:

- Within the member firm.

- To clients as required by applicable law, regulation or standards, including without limitation any breaches of applicable independence regulations.

- To external parties (e.g., regulators) as required by local laws, regulations, or professional standards.

What does this mean for you?

In all cases –whether you are a professional in Audit, Tax, or Advisory – Speak Up and report the suspected or actual non-compliance to your engagement partner.

If you are an engagement partner, you need to:

- Understand the facts and circumstances of the identified or suspected non-compliance with laws or regulations.

- Report the matters to your firm's RMP (except where the matter is clearly inconsequential).

- Avoid alerting the client or third party if you suspect them of wrongdoing.

KPMG's RMP and internal general counsel will determine appropriate next steps.

If you are unsure whether a client or third party is in breach of a certain law or regulation, or whether a matter is clearly inconsequential, always Speak Up and raise the concern with your engagement partner – who can report it to the RMP if required.

Global Informatiom Protection & Data Privacy Fundamentals Trainings FY24

Introduction to the course

This course will give you the fundamental knowledge and key behaviors required to protect our client's information, KPMG information and our reputation.

This course contains 8 modules, and each one should take around 10 minutes to complete:

Scenario 1 - Handling Information Securely

Scenario 2 - Password Security

Scenario 3 - Secure Communication

Scenario 4 - Phishing, Social Engineering & Social Media

Scenario 5 - KPMG IT and Facilities, and use of AI Tools

Scenario 6 - Work Securely Wherever You Are

Scenario 7 - Working Securely With Clients

Scenario 8 - Data Privacy Principles

! You should ensure that you are familiar with KPMG's Information Protection and Data Privacy Policies (in case you have a KPMG account), in addition to completing this course (access your member firm's policies via your member firm portal, or by contacting your local Quality & Risk Management).

Welcome to the Global Informatiom Protection and Data Privacy training

We all need to take steps to protect information, devices, and the workspace - whether at home, in the office, or on the move - to help prevent breaches that could have a significant impact for the business, and for us as individuals. Negative impacts such as:

- ✓ reputational damage
- ✓ business disruption
- ✓ loss of public trust in our firm
- ✓ sanctions or fines from our regulators
- ✓ possible disciplinary action against individuals.

Welcome to the Global Informatiom Protection and Data Privacy training

Getting this right is a key component of our strategy to become the most trusted professional services firm to our clients and the public.

We want to help you make well-informed decisions and do the right thing when it comes to protecting information and privacy - and this course will provide the fundamental knowledge and key behaviors needed for this.

Remember - wherever you are, whoever you're with, whatever you're saying, whatever you're feeling, whatever you're doing….

… Be KPMG Cyber Secure - our reputation depends on it

! If you believe that confidential information and/or equipment used to store such information has been lost, stolen or otherwise compromised, immediately report the matter following KPMG firm's procedures.

Scenario 1 – Handling Information Securely

Scenario 1 – Handling Information Securely

Nia is working on a project for an insurance client.

She's building an application that will review insurance claims handling. The client has just provided the dataset for analysis.

Nia knows she needs to apply a classification level to the dataset, but she's unsure which one to apply, or how to find this out.

She has a deadline coming up, so hasn't got time to look into it now.

Should Nia take time to find the classification details now, or leave it for another time when she's less busy?

Scenario 1 – Handling Information Securely

Should Nia take time to find the classification details now, or leave it for another time when she's less busy?

A. No - she can leave it as her deadline is more important, and it might take too long to find out what the correct level should be.

B. Yes - she should take the time to find out what the correct level should be. She can ask the Information Owner (usually the Engagement Leader) or check if there's an Information Protection Plan (IPP) for the project.

Scenario 1 – Handling Information Securely

Should Nia take time to find the classification details now, or leave it for another time when she's less busy?

A. No - she can leave it as her deadline is more important, and it might take too long to find out what the correct level should be.

B. Yes - she should take the time to find out what the correct level should be. She can ask the Information Owner (usually the Engagement Leader) or check if there's an Information Protection Plan (IPP) for the project.

Scenario 1 – Handling Information Securely

She should take the time to find out what the correct level should be. She can ask the Information Owner (usually the Engagement Leader) or check if there's an Information Protection Plan (IPP) for the project.

KPMG may suffer reputational damage, loss of client business and trust, and fines from regulators if the information was breached as a result of incorrect classification. It's always best to check if you're unsure, rather than guess. It's too risky to get this wrong.

The KPMG Information Owner is responsible for the secure custody, transport and storage of information created or obtained in KPMG, so they would know which classification level to apply. Also, if an Information Protection Plan is in place, this will document the procedures required to appropriately handle all information and data on that project.

Scenario 1 – Handling Information Securely

Nia knows that as this document contains sensitive personal data, it needs to be handled with the utmost care at all times.

If it's not classified correctly, it might be stored in the wrong place, or viewed by unauthorized people.

She's pressed for time, but after a few minutes she manages to find the information she needs on the portal.

She applies the highest classification level - KPMG Highly Confidential.

Later Nia is working on a report for the client.

She needs to save the document somewhere - but where would be best?

Scenario 1 – Handling Information Securely

Where should Nia save the document?

A. She should check with her team which repository they are using to store all project documentation. Or she could check if there are any specific security requirements for the engagement on document storage. These may be documented in an Information Protection Plan (IPP), based on client requirements and the type of information being handled.

A. It's more convenient if she saves it on her desktop, as it provides easy access. She's going to need it soon, so has to be able to find it quickly. And KPMG laptops are updated all the time with security features, so it's not at risk.

Scenario 1 – Handling Information Securely

Where should Nia save the document?

A. She should check with her team which repository they are using to store all project documentation. Or she could check if there are any specific security requirements for the engagement on document storage. These may be documented in an Information Protection Plan (IPP), based on client requirements and the type of information being handled.

A. It's more convenient if she saves it on her desktop, as it provides easy access. She's going to need it soon, so has to be able to find it quickly. And KPMG laptops are updated all the time with security features, so it's not at risk.

Scenario 1 – Handling Information Securely

Her team are likely to be using an internal document management system, as this is the most secure. It's not good practice to save information on your desktop, especially confidential information, as it's more at risk of being lost or stolen. It's better to store it in a secure, KPMG approved repository, as this prevents unauthorized access.

You shouldn't store sensitive personal data or Highly Confidential information on Teams, unless it has been approved by the Engagement Leader. And you should never store KPMG or client information on an external cloud solution like Dropbox, unless this has been approved by the client and the National IT Security Officer (NITSO).

Document Classification: KPMG Public   90

Scenario 1 – Handling Information Securely

Nia knows that the document should be stored in a secure place, and it's likely to be stipulated in the terms of the client contract.

The engagement manager will know more.

She messages her manager to ask which repository the team are using for this project.

The team are using Teams for this project, so she stores the document there.

Then her engagement manager replies that they'd like Nia to give access to the other project team members who may need to work on the data at a later time.

Nia hesitates as she wonders if this is the right thing to do – she wouldn't want anyone to access confidential information about herself, if they didn't need to.

Should she give access to everyone in the team?

Scenario 1 – Handling Information Securely

Should Nia give access to these colleagues?

A.Not before checking again with her manager. The document contains confidential information, so access should be restricted only to those that need to know or use it for their work.

B.Yes - she should do as the manager asks without questioning their instructions. The manager would be aware of the risks of giving too many people unnecessary access.

Scenario 1 – Handling Information Securely

Should Nia give access to these colleagues?

A. Not before checking again with her manager. The document contains confidential information, so access should be restricted only to those that need to know or use it for their work. ✓

B. Yes - she should do as the manager asks without questioning their instructions. The manager would be aware of the risks of giving too many people unnecessary access.

Scenario 1 – Handling Information Securely

If you think that something doesn't sound right then you should always check. It's possible that the manager may be unaware of the full circumstances, or may not have fully considered the risks of giving access to these colleagues.

You can never be too cautious, and your manager would prefer you to highlight security concerns rather than say nothing, which could then result in a serious data breach with severe consequences for KPMG.

Scenario 1 – Handling Information Securely

Nia messages her manager again, suggesting that access should be restricted only to those that need to know or use the report.
Her manager agrees and thanks Nia for taking care to be secure.
Nia gives access only to those team members that need to work with the data.

Scenario 1 – Handling Information Securely

In this scenario you experienced examples of applying the correct classification level, secure storage of confidential data, and secure access rights.

There are important points to consider when handling information securely.

Read the following KEY CONSIDERATIONS to find out more.

Information Classification - KPMG has 3 information classification levels:

KPMG Public

This applies to information that is made **generally available to the public** and may be disclosed without affecting either a client or KPMG. Examples:

- Information on external KPMG websites
- Press releases
- Marketing materials
- Published annual reports

KPMG Confidential

This is the **default classification** and applies to information for which unauthorized disclosure, compromise or destruction would either directly or indirectly have an adverse effect on KPMG, its clients or employees. Examples:

- Most engagement documentation
- Personal information
- Internal information such as policy, HR and finance records
- General administration records

KPMG Highly Confidential

This applies to information which, if disclosed to unauthorized persons, would give access to business secrets, jeopardize the interests of KPMG or its clients, or would be of **serious personal or financial detriment**. Examples:

- Sensitive personal information
- Price and market sensitive information
- Sensitive engagement documentation
- Where a third party impose the highest level of confidentiality
- from April 2024 this category will be re-labelled as KPMG Restricted

Information Protection Plans (IPPs)

What is an Information Protection Plan (IPP)?

It's a tool that can be used to **document the measures and procedures** the engagement/project team can take to appropriately protect and handle information and data for that project. It helps us to meet our client's minimum security requirements, and to ensure that engagement team members understand their individual responsibilities for protecting client information.

Who is responsible for the IPP?

The **Engagement Leader** (as Information Owner) should complete, maintain and manage the IPP. But this can be delegated to another member of the engagement team who has a good understanding of the client engagement and the handling of client information.

The **Engagement Partner** should be responsible for approving the completed IPP, as they have the required seniority and authority.

All **engagement team members** (including contractors) would then be required to comply with the IPP.

Where can I find an IPP template?

Section **15.3.3 of the GQRMM** contains an IPP template.

Retention, Storage and Disposal

It's important to protect documents and client records (KPMG or engagement-related information produced during the course of providing professional services to a client) from **loss, destruction, falsification, unauthorized access and unauthorized release**, in accordance with legislative, regulatory, contractual and business requirements.

Handling hard-copy information

Protect hard-copy information - e.g. **paper copies, print-outs, printed material, files or documents** – whether working at a KPMG office, client site or a remote location:

- Securely store confidential KPMG and client files at all times in **secured, designated areas**, or with KPMG approved offsite storage providers (and keep the relevant inventories up to date).

- Return hard-copy information to **secure storage** as soon as any reviews or reference work has been completed.

- If you need to **send confidential documents securely by post**, make sure you follow your Member Firm's process (e.g. use a locally approved courier).

Retention

Retain records for the right period of time, in accordance with your **Member Firm's Records Retention Schedule**. If documents don't need to be retained, delete them or dispose of them securely, in accordance with your Member Firm's polices and procedures.

Digital storage

- Store records in the **approved document management system** used by your Member Firm (always check and get approval before storing any Highly Confidential materials).

- Don't backup any KPMG device (and the data stored on it) to a **non-approved Cloud service**.

Disposal

Dispose of documents, devices and digital files according to your Member Firm's policies and procedures:

Hard copy documents

- Dispose of in the office in a **confidential waste bin**

- Dispose of at home using your own **cross- cut shredder** (as long as it's compliant with the DIN 66399 security level 4 standard, or higher)

Devices

- E.g. unwanted laptops, USB sticks, mobile devices, hard disks

- Send or hand these in to **ITS**, who will securely dispose of them for you

Emails/digital files

- Check your Member Firm's **Retention Policy** first to ensure they don't need to be retained for longer

- **Manually delete** files and emails that are no longer required
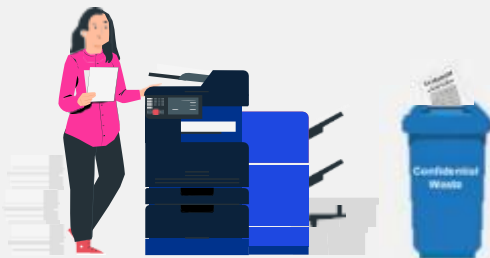
Access Rights and Need to Know

When you're entrusted with confidential or personal information, you have a responsibility to ensure that information is **only shared with someone who also has a business need to know**, and is properly authorized to access it. Just because someone works with KPMG doesn't necessarily mean they need to access personal and confidential information.

To protect confidentiality and better understand what information to share (and with whom):

Avoid mentioning client names or describing details that could identify a specific client

Be mindful who you share or discuss personal or confidential information with, even within KPMG

Make sure information disclosures align with client expectations and the terms of the relevant engagement

Limit access to information only to those people who are authorized to see it, and ensure that you only have access to information you're authorized to see

Confirm that third parties and vendors have a legitimate need and the proper authorization to access personal and confidential information

Document Classification: KPMG Public

Scenario 2 – Password Security

Scenario 2 – Password Security

Alex has just joined KPMG. He needs to set a password to his new log-in account.
He thinks back to his induction where password requirements were discussed.
He's finding it hard to think of one, but realises that his personal Hotmail password would fit the requirements.
He hesitates for a moment, wondering if he should do this.
Should Alex reuse his personal password for his KPMG log-in account?

Scenario 2 – Password Security

Should Alex reuse his personal password for his KPMG log-in account?

A. Yes it's fine to reuse a personal password, as long as it fits KPMG's requirements on length and strength.

B. No, you should never use the same password for your KPMG log-in account that you use for personal accounts.

Scenario 2 – Password Security

Should Alex reuse his personal password for his KPMG log-in account?

A. Yes it's fine to reuse a personal password, as long as it fits KPMG's requirements on length and strength.

B. No, you should never use the same password for your KPMG log-in account that you use for personal accounts. ✓

Scenario 2 – Password Security

You should always use a unique password for your KPMG accounts. Otherwise, if a hacker steals or guesses your personal password, they could potentially gain access to KPMG's network and systems, as well as your KPMG account.

Scenario 2 – Password Security

Alex remembers from the induction that you're not supposed to use the same password for your KPMG log-in that you use for personal accounts.

If a hacker steals or guesses his personal password, they'd also have access to his KPMG account.

He looks around the room and sees three things he can use to devise his KPMG password.

He comes up with a long, strong password that will be easy to remember.

Scenario 2 – Password Security

Secure passwords must:

✓ Contain a minimum of 8 characters

✓ Use a mixture of upper-case and lower-case letters, numbers, and/or special characters

✓ Be changed at least every 90 days

It is advisable to make your password something you can remember - try to think of a phrase containing three unrelated words, then make this meet our password requirements.

For example:

bird   spoon   winter

converts to:

bi£dSpoonwint%r

Document Classification: KPMG Public

Scenario 2 – Password Security

Later, Alex is chatting to his colleague, Sanjiv, about a data cleansing tool his team are using on their engagement.

Sanjiv had previously requested to download this handy app to use for his client work, but his request was denied.

He asks Alex if he will share his credentials, so he can use the app from Alex's account.

Alex isn't sure if he's allowed to share his KPMG credentials - he definitely wouldn't share his personal credentials with anyone.

How should he respond to Sanjiv?

Scenario 2 – Password Security

How should Alex respond to Sanjiv?

A. Alex should tell him that he cannot share his log-in credentials under any circumstances. There are just too many risks in doing this.

B. He should share his credentials to help his colleague out with his engagement. It's not a risk as they work in the same department, and the app has been approved for use.

Scenario 2 – Password Security

How should Alex respond to Sanjiv?

A. Alex should tell him that he cannot share his log-in credentials under any circumstances. There are just too many risks in doing this. ✓

B. He should share his credentials to help his colleague out with his engagement. It's not a risk as they work in the same department, and the app has been approved for use.

Scenario 2 – Password Security

Alex is accountable for all activity that occurs in his KPMG account. So if Sanjiv logs in as Alex, and performs unauthorized activities (e.g. processing client data in a tool that hasn't been approved for use on that engagement), Alex would also be held responsible for the breach of contract.

Just because an app has been approved for use in one client engagement, it may not be approved for a different engagement, even within the same department (e.g. because each client may have unique security requirements, or because there is a higher risk if more sensitive information is involved).

Other risks include:

- Sanjiv may be able to access KPMG or client information that he's not authorized to view, or KPMG systems he's not supposed to access (e.g. if Alex has any privileged system or network access).

- He may perform unauthorized activities (such as making alterations to work) which would be attributed to Alex.

- Sharing access to third-party provided software may breach the terms of the licence agreement.

Scenario 2 – Password Security

Alex tells Sanjiv that he can't share his password with anyone.

He explains that he's accountable for all activity that occurs in his KPMG account, including any activity that may lead to a data breach. It's too much of a risk.

Sanjiv understands Alex's reasons - he'll speak to his engagement manager again about the possibility of using the app.

Scenario 2 – Password Security

In this scenario we learnt about setting a strong, unique password, and not sharing credentials.

Read the key things to consider about password security by Selecting KEY CONSIDERATIONS.

Passwords

It's essential to create **strong passwords** to guard against the threat of cybercriminals who are looking to gain access to KPMG's network and systems. A weak password can be guessed very quickly e.g. password123 could be cracked in seconds.

However a complex password (or passphrase) that is **hard to guess but easy to remember** may take months or more to crack, by which time the password on your KPMG device will have been changed as per policy.

These are the minimum password requirements (but check your Member Firm policy as they may have stricter requirements):

A) **Password minimum length** — Passwords must have at least 8 characters.

B) **Password complexity** — Passwords must contain any three of the following four qualities: Uppercase characters, Lowercase characters, Alphanumeric characters and special characters (e.g. #*&% etc.).

C) **Password change period** — Passwords must be changed at least every 90 days

Strong Password	Weak Password
footBallMonkey2shaDow@	password123
roCket%time8gasolinE	IloveUnited
Tomato&holidaY29parent	Summer2023
jIgsaW73quicKly$kNife	P@$$w0rd

To make your password memorable, a good tip is to use 3 random words (e.g. swipe, house, paper) and insert special characters and numbers: **sWipe4house%paper**

Avoid commonly used words like **"p@55word"** and **"welcome"** and avoid common phrases like **"IloveMyDog"**, or words associated with you that might be easily guessed e.g. family, pet names, company name, favourite film or sports team, your username

Passwords

Remember that you're accountable for **all system activity** that occurs using your KPMG assigned credentials (login/sign on details and passwords).

- The passwords you use for KPMG systems **must be unique**, and mustn't be used for any other (e.g. personal) accounts.

- Protect all passwords that are used to access KPMG devices – **don't share them** or write them down.

- Take care to secure all associated access mechanisms such as **PINs, tokens, and access devices** from loss and disclosure.

Check if you have an email address – work or personal - that's been compromised in a data breach, by visiting external website **https://haveibeenpwned.com/**.

If it has, change your password immediately and contact your local ITS Helpdesk.

Scenario 3 – Secure Communication

Scenario 3 – Secure Communication

Li has just arrived in the office when she receives a message from her colleague Elena.

Elena is briefing the Engagement Leader soon, so Li wants to reply quickly.

But she's unsure if they should be discussing details of a client engagement on WhatsApp.

How should Li respond to Elena?

Scenario 3 – Secure Communication

How should Li respond to Elena?

A.Li should give her a brief update in a WhatsApp reply, as Elena needs the information fast. It's fine as long as she doesn't disclose any confidential information.

B.Li should use an approved communication channel (such as Exchange / Outlook, MS Teams) to send the message.

Scenario 3 – Secure Communication

How should Li respond to Elena?

A. Li should give her a brief update in a WhatsApp reply, as Elena needs the information fast. It's fine as long as she doesn't disclose any confidential information.

B. Li should use an approved communication channel (such as Exchange / Outlook, MS Teams) to send the message. ✓

Scenario 3 – Secure Communication

WhatsApp is fine for chatting to your colleagues about personal things, but you shouldn't use it for business-related communication (especially when discussing a confidential client engagement), as it isn't a KPMG approved communication app. Unapproved apps may not be secure and may put us at risk of a data breach. There have even been instances where malicious actors have set up fake profiles pretending to be senior colleagues, asking for confidential information to be disclosed.

! Using one may also violate the firm's retention standards, or cause information to cross borders and breach local data privacy regulations.

It might take longer to use an approved method, but it's better to be secure and help to prevent sensitive information from falling into the wrong hands.

Scenario 3 – Secure Communication

Li realises that WhatsApp isn't a KPMG approved communication app, so shouldn't be used for any business-related conversations.

She decides the best thing to do is to reply via Teams.

It will only take a few seconds longer, and will mean that the information is at less risk of being intercepted by a third party.

Later, Li gets a message from the engagement leader Jakob, asking her to send a summary of her report to Marcus at the client.

She types out an email to the client.

Li hesitates - this is valuable market-sensitive information that she's about to send externally. She's unsure if it's ok to include it in the body of an email.

How should Li ensure that the information is secured properly before emailing the client?

Scenario 3 – Secure Communication

How should Li ensure that the information is secured properly before emailing the client?

A. Li needs to take an extra step and encrypt the sensitive information using an approved tool (e.g. WinZip), before attaching it to the email.

B. Li can send the information in the body of the email, as long as it's sent via a KPMG approved email tool (e.g. Outlook).

Scenario 3 – Secure Communication

How should Li ensure that the information is secured properly before emailing the client?

A. Li needs to take an extra step and encrypt the sensitive information using an approved tool (e.g. WinZip), before attaching it to the email. ✔

B. Li can send the information in the body of the email, as long as it's sent via a KPMG approved email tool (e.g. Outlook).

Scenario 3 – Secure Communication

Information about an acquisition is confidential, and needs protection when being sent externally. If you're sending confidential information or data in an attachment to a client or other third party, it must be encrypted using an approved product such as WinZip. The encryption password must then be sent via a separate method (e.g. telephone call or SMS), as this minimizes the risk of a malicious third-party intercepting both communications and accessing the information.

! Whenever you send Confidential or Highly Confidential information to a client, always check first that the client has approved the method of communication (e.g. email) that you will be using. Check with the Engagement Leader or Manager, or check the engagement IPP (Information Protection Plan), if one is in place.

Scenario 3 – Secure Communication

Li knows that the information is too sensitive to be sent unprotected.

If she were sending confidential information about herself by email, she'd want to protect it as much as possible from unauthorized disclosure.

She decides to paste the summary into a Word document and encrypt it instead.

Now she just needs to add Marcus's name to the address field and hit send. She hurries, as she's late for coffee with Elena.

Li has accidentally sent the email to one of her old clients, Martin Dawson.

She panics at first, but then remembers that the information was protected by encryption, and he doesn't have the password to open the file.

She can fix this by asking Martin to delete the email and confirm when he's done it.

Li isn't sure she's done everything she needs to in this situation.

What else does she need to do?

Scenario 3 – Secure Communication

What else does Li need to do?

A. She needs to report this immediately as a data breach.

B. She needs to inform her engagement leader at their next catch-up meeting. It doesn't need to be reported as a data breach as Martin had no way of reading the encrypted details, and she trusts him to have deleted the email. It would just cause unnecessary alarm, and may harm the client relationship.

Scenario 3 – Secure Communication

What else does Li need to do?

A. She needs to report this immediately as a data breach. ✓

B. She needs to inform her engagement leader at their next catch-up meeting. It doesn't need to be reported as a data breach as Martin had no way of reading the encrypted details, and she trusts him to have deleted the email. It would just cause unnecessary alarm, and may harm the client relationship.

Scenario 3 – Secure Communication

Even though Martin doesn't have the password to read the encrypted details in the email, Li should still report this incident immediately. The person investigating can then decide on the most appropriate course of action.

It's important to report actual or suspected security incidents promptly via your local reporting channel (e.g. the IT service desk, the National IT Security Officer (NITSO) or Privacy Liaison (PL)), so that they can respond quickly to minimize any damage to our operations and reputation caused by a breach.

You shouldn't inform anyone else, including the engagement leader, client, or other colleagues, without consulting with your local Risk Management team. If you've accidentally sent an email containing confidential information to the wrong address, get approval from your local Risk Management team to contact that person and ask them to delete the email (and get written confirmation that this has been done).

Scenario 3 – Secure Communication

Even though Li feels embarrassed to admit she's made a mistake, she knows that the most secure thing to do is to report this as a data breach immediately.

That way, the person investigating can decide whether more needs to be done, and quickly take action to minimize any damage.

Scenario 3 – Secure Communication

In this scenario we learnt about using secure communications channels, including messaging apps and encrypted emails, plus what to do if you send confidential information to the wrong recipient.

Read the key things to consider about communicating securely by Selecting KEY CONSIDERATIONS.

Approved Communications Tools

KPMG provides users with **chat facilities and conferencing services** to facilitate improved communication and collaboration between KPMG personnel.

You should only use KPMG-approved electronic communication methods (e.g. **Exchange/Outlook, MS Teams, SharePoint Online**) for business-related communication and collaboration. The Resources section has a link to the Global 'External Collaboration' portal which contains more information on which tools are approved for use.

Non-approved tools (such as WhatsApp, WeChat, various social media tools and blogs, DropBox, personal OneDrive, Google drive, personal webmail) should never be used for KPMG, client or engagement-related communications, unless expressly approved by the National IT Security Officer (NITSO). This is because:

- they may **not be secure** and may put us at risk of a data breach.
- they may **violate the firm's retention standards**, or cause information to cross borders in jurisdictions where local data privacy regulations prohibit such transfers.

Remember your responsibilities when using these services

As with all forms of electronic communication, always **take care to ensure that you maintain client confidentiality and respect individual privacy** at all times. You have a general responsibility to act in a way which is both proper and legal.

Use of Email

Email is a business tool – use it appropriately

It's important to understand the risks associated with the use of email for business purposes - including the exposure of confidential information. Email is not inherently secure and shouldn't be considered private - it can be **forwarded, intercepted, printed, and stored** by others.

Think twice before you click "Send"

Always **double check recipients**, especially when emailing externally. It's good practice to disable autocomplete or set a send delay.

Use the **"Blind CC"** feature when distributing a message to a large list, to keep each recipient's email address private.

Don't **exchange** confidential information with a client over email, unless that client has explicitly authorized the use of email for correspondence.

Don't **forward** business email messages to your personal email account, or use your personal email account for KPMG business purposes.

Similarly, avoid using your KPMG email address for **non-business purposes**.

Minimize the information on your **out-of-office message** – never disclose any information that could be misused by an unintended recipient.

Use of Email

What happens if I inadvertently send an email to the wrong person?

Report the data breach **immediately** as per local procedures, for example by notifying the ITS Helpdesk, so that the necessary action may be taken.

Also, **contact the unintended recipient**, explain that you've sent them something in error, and ask them to delete it and confirm by email that they've done so.

When sending confidential information/data in an attachment to a client or other third party, it **must be encrypted** using an approved product (e.g. WinZip).

Passwords should conform to KPMG minimum requirements, and must be sent in a separate communication (via a different medium e.g. a text message or telephone call).

Conference calls and virtual meetings

If you're leading a virtual meeting or conference call in which people will discuss sensitive or confidential information, it's important to understand the risks involved:

Participants

Make sure that only the **intended participants** are present, and that no uninvited guests are listening in on the call.

Voice recordings

Consult your member firm policies to understand what's allowed with regards to **recording conversations and conferences**, e.g. disclose the intention to record a meeting or discussion at the start of the proceedings.

Surroundings

Be aware of your surroundings and **avoid being overheard** by moving to a more private area.
If you can't avoid being overheard, let other participants know and take care in what you say.

Smart devices

When working from home, ensure that you aren't near any **smart speakers or voice activated assistants**, or ensure that they're switched off.

Conference codes

(If still in use) Remember to keep your conference call leader code **private**, distribute the participant code only to individuals who need to know it, and change your codes periodically.

Scenario 4 – Phishing, Social Engineering & Social Media

Scenario 4 – Phishing, Social Engineering & Social Media

Ade and his team have just won a major new piece of work.

He's proud of his team, and wants to congratulate them on their achievements on social media.

Ade pauses - his account can be viewed by the public, and he might be giving away too much detail on the client work.

He wouldn't want to share too much detail about his personal life on social media.

How much detail should Ade share about the new client on social media?

Scenario 4 – Phishing, Social Engineering & Social Media

How much detail should Ade share about the new client on social media?

A. He should post full details about his KPMG role and latest client project, because success stories will enhance the KPMG brand.

B. He should keep details of the work he does and client projects to a minimum
e.g. don't mention the client by name or the nature of the engagement work.

Scenario 4 – Phishing, Social Engineering & Social Media

How much detail should Ade share about the new client on social media?

A. He should post full details about his KPMG role and latest client project, because success stories will enhance the KPMG brand.

B. He should keep details of the work he does and client projects to a minimum
e.g. don't mention the client by name or the nature of the engagement work.

Scenario 4 – Phishing, Social Engineering & Social Media

When you use social media, it's important to be aware of the potential risks and be careful about the information you share – particularly as content you post is likely to be seen by more than just your intended recipients.

! If you're creating an online profile or resume, you should never share too much detail about your KPMG role and work activities. This is especially important if you access confidential or commercially sensitive information, or if you have privileged account access.

Sharing too much detail may breach confidentiality, violate others' privacy, or leave you vulnerable to social engineering attacks (where people are targeted by phishing emails, crafted using information shared on social media or other publicly available data).

Always review your Member Firm's information security policies and social media guidelines before posting.

Scenario 4 – Phishing, Social Engineering & Social Media

Ade reconsiders sharing this amount of detail, as it would breach client confidentiality.

He wants to set a good example to his team on being secure, so he edits the post to remove details about the client and nature of the work.

Can you identify where details should not have been shared on social media?

Document Classification: KPMG Public

Can you identify where details should not have been shared on social media?

Scenario 4 – Phishing, Social Engineering & Social Media

Ade is on a Teams call to discuss his new engagement, when he receives an email.

It appears to be an expenses query from the internal Finance team.

The email contains some red flags/cues that indicate it may not be genuine.

Ade is busy with the meeting but is curious to learn more about the issue with his expenses, so he Selects on the attachment before reading the email properly.

The attachment opens up a loading bar, instead of a document.

A ransom message appears.

Ade has inadvertently executed malware in the form of a ransomware attack, that could now spread throughout the firm's network.

The message is demanding funds to be paid into a cryptocurrency wallet to restore encrypted data, and prevent it from being leaked.

What should Ade do next?
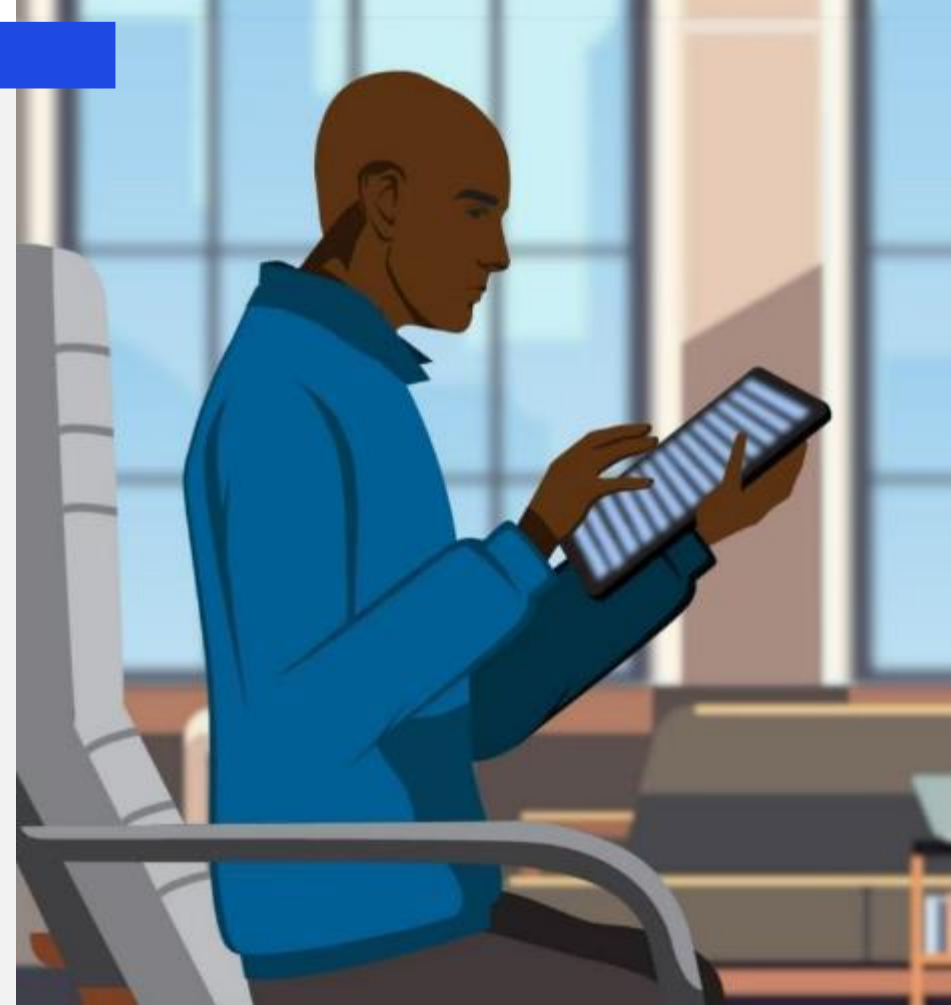
Scenario 4 – Phishing, Social Engineering & Social Media

What should Ade do next?

A. Disconnect from the Wi-Fi immediately and then report the attack as a security incident.

B. Quickly restart his computer, and then delete the email.

Scenario 4 – Phishing, Social Engineering & Social Media

What should Ade do next?

A. Disconnect from the Wi-Fi immediately and then report the attack as a security incident. ✓

B. Quickly restart his computer, and then delete the email.

Scenario 4 – Phishing, Social Engineering & Social Media

As this is a ransomware attack that is already underway, he needs to act quickly by disconnecting from the Wi-Fi and then reporting the attack on a separate device (it's a good idea to keep the phone number of your local reporting channel stored in your mobile device, in case of such incidents), or asking a colleague to report on his behalf.

! Don't shut the device off, as that will negatively impact the forensic recovery of volatile data and malware analysis.

It's important not to try to deal with this yourself – let colleagues used to dealing with these incidents guide you on the next steps to follow.

Scenario 4 – Phishing, Social Engineering & Social Media

As this is a ransomware attack that is already underway, Ade needs to act quickly by disconnecting from the Wi-Fi connection, and then reporting the attack as a security incident. The person investigating will guide Ade on the next steps to follow.
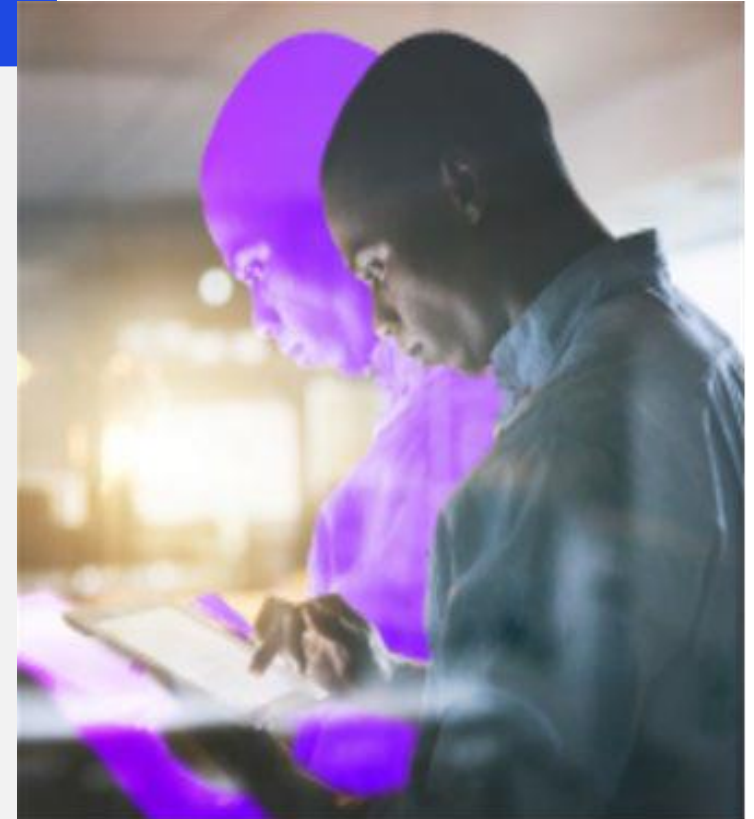
Scenario 4 – Phishing, Social Engineering & Social Media

In this scenario you experienced:
- examples of oversharing on social media
-examples of phishing and social engineering attacks
- how to deal with a ransomware attack.

Read the key things to consider about phishing, social engineering & social media security by Selecting KEY CONSIDERATIONS.

Phishing

Phishing is a form of cyberattack where an attacker sends a fraudulent message designed to trick you into:

- **Revealing personal or sensitive information**, such as your KPMG username, passwords, personal identity numbers, or bank details

- **Opening an attachment** which deploys malicious software onto your device

- **Clicking on a link** which takes you to a fake website

Phishing emails: example of what to look out for

Document Classification: KPMG Public

Phishing

How to spot a phish?

As employees of KPMG **you are a target**, due to the nature of the firm's work and the high-value data we process.
You can reduce the risk of becoming a victim by paying close attention as you review email and text messages. Look out for:

- Emails that are **not addressed to you personally** e.g. 'Dear Customer'.

- An email asking for an **invoice to be paid** or information to be provided.

- An email that invokes **a unusual/out-of-context sense of urgency** or is vague and impersonal.

- **Spelling and grammar** mistakes.

- Emails containing a **link to a webpage or file** you're not familiar with. Don't click on it – instead hover your cursor over the link to show the URL. This is a good way to ascertain whether the email is genuine or not.

- If you receive a file and you don't know what it is – don't open it. In particular, email attachments with ".scr," ".com" and ".exe" file extensions may contain **malware or a virus**.

- An **email address that's not quite correct** – it may use the name of someone you know or a familiar company but will differ slightly. Check the email address to identify if it's authentic.

- An email that claims to **activate or suspend a financial account**, change a password or payment technique, or that prompts for personal or banking details. Validate the source and the site before providing any personal or business information.


If you receive a suspected phish direct to your inbox, **don't click on any links or open any attachments contained in the mail**. And don't forward the email to any colleagues.

If your Member Firm has a **phish reporting button** in Outlook, use this to report the phish. Otherwise, follow the reporting process in your Member Firm e.g. contact your ITS Helpdesk.

Social Engineering

What is Social Engineering?
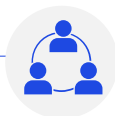
Social engineering is a technique used to **exploit trusted relationships** and to prey on the better qualities of human nature, such as our tendency to be helpful - to trick **you into disclosing valuable information** about yourself, or the firm.

Never provide personal details or confidential information about yourself, your colleagues, the firm, or our clients to someone if you're not sure whether they're authorized to receive it.

Confirm that the person has the right to ask for this information, and that they are who they say they are.

Look out for such attacks

- When they launch their attack, they'll pose as a **trusted source** and may address you by name to add an air of authenticity.
- They may approach you via **social networks** like LinkedIn, offering a business or public speaking opportunity as a way of gathering confidential information.
- Their approach may be via a **personal interaction**, such as a telephone call or face-to-face encounter.
- They may ask for the **names of colleagues** at KPMG, or for an actual KPMG directory.
- **"Spear phishing"** emails target specific people, using information about potential victims harvested from social media or other publicly available data e.g. the conferences you attend, your professional areas of interest etc.)

!

Video and audio Deepfakes – artificial media replacing a person with another's likeness or 'cloned' voice - can be used in social engineering scams, fooling people into thinking they received instructions from someone they trust, asking to transfer money into a bank account.

Avoid being scammed by a **phone call, email, SMS or social media message** from an attacker impersonating someone you know. Always check separately with that person before you transfer any money.

Social Media

When you use social media, it's important to be aware of the **potential risks** and be careful about the information you share – particularly as content you post is likely to be seen by more than just your intended recipients.

We all have a personal and professional responsibility to **protect client confidentiality**, show **respect** for other people and their privacy, and maintain the highest regard for KPMG's **reputation and values** when using internal or external social media.

Review your Member Firm's information security policies and social media guidelines before posting. In addition, abide by the following best practice:

- Familiarize yourself with each site's **privacy policy and security settings**, and make adjustments as appropriate.

- Don't post or link to materials that are **defamatory, harassing or indecent**.

- Don't use the same **password** as you do on the KPMG network or other sites, as if one site is compromised, your exposed password can be used to access your accounts on other sites. And don't use your **KPMG email address** on social networks, unless required for professional purposes.

- When creating an online profile or resume, don't share too much detail about your **KPMG role and work activities** - especially important if you access Highly Confidential or commercially sensitive information, or have a privileged account.

- Don't share any information that may cause damage to **KPMG's reputation**, and don't offer advice or provide information that could be interpreted as official business advice from KPMG.

Scenario 5 – KPMG IT and Facilities, and use of AI Tools

Scenario 5 – KPMG IT and Facilities, and use of AI Tools

Sofia has been busy all morning, but now it's lunchtime, and she takes a well-earned break.

During her lunch break she likes to catch up with the news and browse the internet.
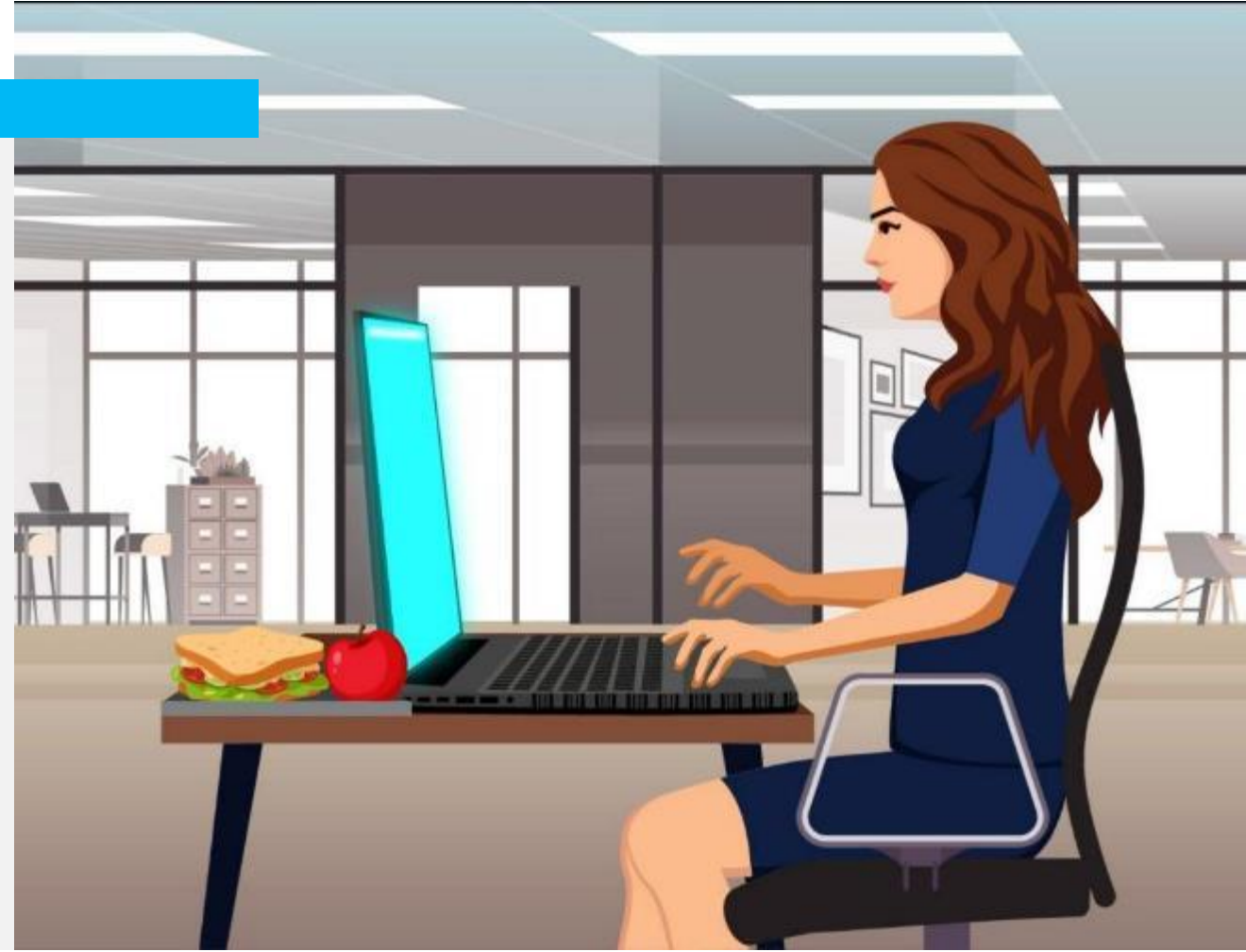
Which of these websites are appropriate to access on a KPMG device?

Gambling Websites

Facebook

Google

Wikipedia

Pornographic websites

Websites containing details of or encouraging illegal activities

Answer:

APPROPRIATE TO ACCES

Facebook

Google

Wikipedia

INAPPROPRIATE TO ACCES

Gambling Websites

Pornographic websites

Websites containing details of or encouraging illegal activities

Scenario 5 – KPMG IT and Facilities, and use of AI Tools

Sofia also likes to check-in on her online business. She makes jewellery in her spare time, and sells it via an online marketplace.

She's just started using a new application that promotes her listings across social media, and should help to grow her sales.

Sofia uses this app on her personal laptop at home, but she thinks it would be handy to download it onto her work laptop as well.

She hesitates as she's unsure if it's ok to download an app for personal use to your KPMG laptop.

Should Sofia go ahead and download the app?

Scenario 5 – KPMG IT and Facilities, and use of AI Tools

Should Sofia go ahead and download the app?

A. No, as she hasn't obtained authorization to download the app.

B. Yes, as she only plans to access it during her lunchbreak, so it won't interfere with her work. Reasonable personal use of KPMG devices is allowed.

Scenario 5 – KPMG IT and Facilities, and use of AI Tools

Should Sofia go ahead and download the app?

A. No, as she hasn't obtained authorization to download the app. ✓

B. Yes, as she only plans to access it during her lunchbreak, so it won't interfere with her work. Reasonable personal use of KPMG devices is allowed.

Scenario 5 – KPMG IT and Facilities, and use of AI Tools

If you want to install new software onto a KPMG device, you need to get approval from your local ITS (who may consult with the National IT Security Officer (NITSO) or local Risk Management team), and provide a valid business case. Unapproved software could pose a threat to KPMG's network and systems (e.g. if it contains malicious code that could cause information exfiltration or data loss).

! And although reasonable personal use may be allowed (subject to local Member Firm rules), you shouldn't use KPMG systems or devices for personal benefit (e.g. running your own business), or install software for personal use on KPMG devices (unless this is specifically permitted by your member firm).

It should also be noted that KPMG personnel would need to contact the Ethics and Independence team regarding obtaining independence clearance, if they want to run their own business outside of KPMG working hours.

Scenario 5 – KPMG IT and Facilities, and use of AI Tools

Sofia thinks it's better to keep her personal business and work separate. She can download the app to her personal mobile phone instead, if she needs to work on it at lunch.

Later she starts to pack up to go home. She plans to do some work over the weekend, but doesn't want to carry her laptop all the way home. She decides to save the documents she's been working on to an encrypted USB stick.

Now Sofia can finish her work at home, on her personal device.

But she's unsure if she should do this – the files she's taking home contain confidential HR data on KPMG employees. Perhaps she should seek permission first?

Does Sofia need to seek permission to use an encrypted USB stick to transfer confidential information?

Scenario 5 – KPMG IT and Facilities, and use of AI Tools

Does Sofia need to seek permission to use an encrypted USB stick to transfer confidential information?

A.No, it's not necessary as this is not too much of a risk. The device is encrypted and will only contain confidential KPMG information, not confidential client or KPMG Highly Confidential information.

B. Yes, she should seek authorization if she wants to use a USB stick to transfer KPMG confidential information to her personal device to work on.

Scenario 5 – KPMG IT and Facilities, and use of AI Tools

Does Sofia need to seek permission to use an encrypted USB stick to transfer confidential information?

A. No, it's not necessary as this is not too much of a risk. The device is encrypted and will only contain confidential KPMG information, not confidential client or KPMG Highly Confidential information.

B. Yes, she should seek authorization if she wants to use a USB stick to transfer KPMG confidential information to her personal device to work on. ✓

Scenario 5 – KPMG IT and Facilities, and use of AI Tools

! You should never transfer or store KPMG or Client confidential information on any personally owned or third-party equipment or service, without the authorization of your Member Firm's IT Services (ITS), the National IT Security Officer (NITSO) and local Risk Management.

The use of USBs is positively discouraged, but if there is no alternative you should only use a KPMG approved device encrypted with an approved solution. And you should take care if transporting confidential information, as small portable storage devices can be easily lost, stolen or misplaced. Such an incident could end up being reported in the media, and may result in significant fines or even professional censure, which would damage KPMG's brand and reputation.

Scenario 5 – KPMG IT and Facilities, and use of AI Tools

Sofia speaks to her manager about this. Her manager tells her not to take the files home, but to finish her work next week in the office, and enjoy her weekend.

Scenario 5 – KPMG IT and Facilities, and use of AI Tools

In this scenario you learned about:
-which internet sites are appropriate to access on a KPMG device,
-rules around installation of software and using KPMG devices for personal use, and
- appropriate use of removable storage devices.

Select KEY CONSIDERATIONS to find out more about using KPMG IT and facilities securely, and appropriate use of AI tools.

Use of the Internet

When you access the Internet or communicate electronically using KPMG's IT resources, it's vital that you **exercise good judgment** to ensure that you don't compromise the reputation of KPMG.

You should never **access, distribute, create or post inappropriate content** when using KPMG devices. Both you and your Member Firm could be subject to legal action, fines, reputational damage or other measures if you're caught doing so.

Inappropriate content includes: any form of written materials, photographs, images or video content, or links to Internet sites that could be considered offensive, illegal, threatening, or otherwise unsuitable in a professional environment (e.g. racial or sexual harassment, defamatory material, unsolicited commercial or political messages).

You should also never access and/or interact with inappropriate websites (unless required for business reasons):

Gambling websites

Websites containing details of or encouraging illegal activities

Pornographic websites

Other websites that may damage KPMG's reputation

Other categories of websites that may present a risk because of a known threat, as notified by the National IT Security Officer (NITSO) or local ITS

Using Approved Software

Approved software is software that's been **reviewed and approved** to use for business purposes on KPMG issued devices. KPMG devices come with a standard suite of approved software that's been risk-assessed, to ensure it poses no threat to KPMG's network and systems (e.g. to ensure it doesn't contain malicious code that could cause information/data exfiltration or data loss).

If you want to **install new software** onto a KPMG device, you need to get approval from your local ITS (who may consult with the National IT Security Officer (NITSO) or local Risk Management team), and provide a valid business case.

Don't assume that because a certain software has been approved for one **project/engagement**, it is fine to use it for your project - the risks may be completely different e.g. regarding the sensitivity of the data to be held in a certain tool.

If you've already installed software that hasn't been assessed and approved yet, **remove it immediately** until approval is granted (or the NITSO may suggest an approved alternative that you can use instead).

If you've installed new software for client work, make sure you **remove the software as soon as it's no longer required**, so that your device is restored to a standard KPMG configuration.

Using Approved Software

Non-Approved third party services

Third party services such as DropBox, personal OneDrive, Google drive, personal webmail, WhatsApp, Siri and Google Translate, **must not be used** to handle or process KPMG or client information, without the explicit approval of the local NITSO.

Generative AI

The use of any AI service or tool is considered a third party service and as such is **prohibited by global policy unless explicitly approved** by the member firm NITSO.

Member firms considering the use of generative AI services and/or tools (including for example ChatGPT, Bard and Dall_E2) must first consult with their NITSO (in conjunction with local Risk Management), and follow **the risk assessment process** in the member firm, as appropriate for the proposed use case.

Use KPMG's IT Resources and Facilities Securely

Personal equipment

If your local member firm supports a **Bring Your Own Device (BYOD) program** for laptops or mobile devices (tablets or smart phones), ensure you comply with all local policies and practices surrounding the registration and use of your device for KPMG purposes. Only backup KPMG data from the laptop or mobile device onto KPMG provided or approved storage.

Third party equipment

Don't transfer or store KPMG Confidential information on any **personally owned or third party equipment or service**, without proper authorization e.g. from IT Services (ITS), the National IT Security Officer (NITSO) and/or local Risk Management. If approval is given, take the necessary steps to ensure information is adequately protected against loss or unauthorized access.

Business versus personal use

Personal use of KPMG IT and information assets may be allowed by member firms (subject to local member firm rules), as long as it's **reasonable** and doesn't breach any KPMG International or local policy:

- Ensure you don't consume **excessive resources** (e.g. with long term storage of personal files on KPMG devices/servers)
- Don't use KPMG systems for **personal benefit** (e.g. running your own business)
- Ensure personal use doesn't interfere with individual **productivity** or impede any KPMG business activity
- Don't install **software for personal use** on KPMG devices (unless this is specifically permitted by your member firm)

Use KPMG's IT facilities and resources securely

Only use **KPMG devices** to store and process KPMG and client information in our custody.

Don't attach any **unauthorized devices** to the KPMG network, or activate unauthorized services (e.g. wireless hot spots).

Connect your KPMG laptop to the KPMG network regularly, to install **security patches and software updates.**

Contact your local ITS Helpdesk if the **security software or features** on your laptop are not up to date or not functioning properly.

Don't attempt to change or disable any **configuration and settings** on KPMG provided hardware or software.

Only take KPMG devices to the ITS Helpdesk to be repaired and maintained – never to an **external IT repair shop.**

Don't ship KPMG devices without implementing appropriate protection (e.g. use an **approved courier**).

If your member firm allows the use of **encrypted storage devices**, only use a password-protected device approved by KPMG.

If you want to **record an online meeting**, ensure you only use approved applications and devices for the recording.

Always keep KPMG-issued devices or removable media **secured when in the office or at a remote location**.

Mobile Devices and Apps

Follow these guidelines on the safe use of mobile devices, to help prevent the exposure of KPMG, client and your personal information and data to the risk of breach or loss:

Only use KPMG approved mobile devices to access KPMG information and systems.

Don't edit or store confidential KPMG or client documents on a personal device.

Consider whether you need to store any personal data on a KPMG device - KPMG reserves the right to 'remote wipe' any mobile device used for KPMG purposes, which may involve the loss of such data.

Never use 'jail-broken,' 'rooted' or similarly compromised devices for KPMG purposes.

Don't change or disable any configuration and settings on your KPMG mobile device.

Choose a hard to guess device password – avoid the use of repetitive numbers and letters, or easily-guessed sequences.

Update your software regularly – installing the latest version of the operating system and applications will help protect your device from most known threats.

Only give your KPMG device to your local ITS for repairs, and never to an external store e.g. an Apple shop.

Protect your device when traveling – keep it with you whenever possible, and at all other times keep it securely stored.

Only **download applications** from a trusted source, such as the official Apple or Google app stores.

Keep it safe at all times

Lock your screen whenever you leave your mobile device unattended for a short period
- at home or in a KPMG office.

Lock it away when not in use for a longer period.

Report any lost or stolen device promptly in accordance with local procedures or policies.

Scenario 6 – Work Securely Wherever You Are

Scenario 6 – Work Securely Wherever You Are

Zainab is working at home this morning, before heading into the office later in the day.

Can you identify the security risks of working at home?

Scenario 6 – Work Securely Wherever You Are

1. She is taking a confidential work call on her mobile, within earshot of other people in the room
2. An active smart device is next to her
3. A man is behind her, looking at details on the screen of her laptop
4. The Wi-Fi router password is written on a post-it note
5. A document marked 'confidential' has been left on the worktop
6. There is a document marked 'confidential' in the waste bin
7. A storage device has been left on a table by the door

Scenario 6 – Work Securely Wherever You Are

Zainab decides to grab some lunch in a nearby coffee shop, on her way into the office.

Can you identify the security risks of being out and about?

Scenario 6 – Work Securely Wherever You Are

1. She is having a confidential conversation on her mobile within earshot of others
2. The server and customer may be able to overhear a confidential work conversation
3. You can see details on an unattended KPMG laptop without a privacy screen
4. There is a document marked 'confidential' on the table next to the laptop
5. There is a mobile phone left on the table
6. There is a laptop bag under the table with confidential documents showing
7. There is a sign in the café displaying the public Wi-Fi

   network name and password – avoid connecting to public Wi-Fi as it may not be secure

Scenario 6 – Work Securely Wherever You Are

Zainab arrives at the KPMG office for her afternoon workshop.

Can you identify the security risks in the KPMG office?

Scenario 6 – Work Securely Wherever You Are

1. A person without an ID badge is trying to enter the office behind Zainab
2. A laptop has been left unattended on a desk, with the screen unlocked
3. A log-in ID and password are visible on a post-it note stuck to a desk
4. Confidential documents have been left inside an unlocked cabinet
5. A mobile device has been left unattended on a desk
6. Two people are having a confidential conversation within earshot of colleagues
7. Confidential information about a client project has been left on a whiteboard
8. Documents marked 'confidential' have been left unattended on a printer
9. A confidential document has been disposed of in a general waste bin instead of the secure disposal bin next to it

Scenario 6 – Work Securely Wherever You Are

In this scenario you learned about the information security risks of working at home, in the office and on the move.

Read the key things to consider about working securely wherever you are by Selecting KEY CONSIDERATIONS.
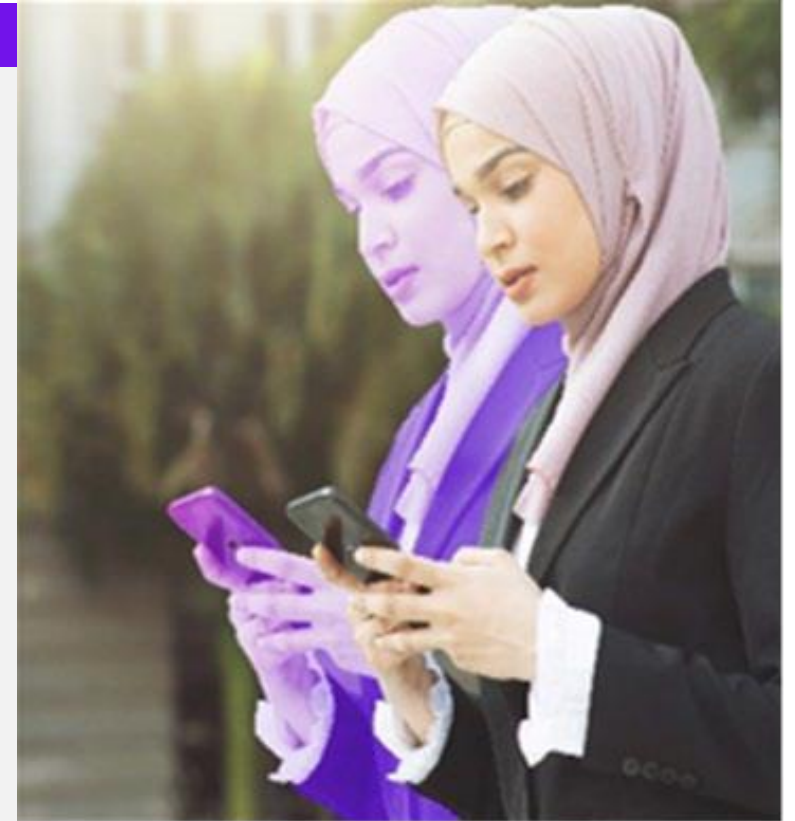
Work Securely at Home

We all have an important role to play in ensuring that **information and devices are kept safe** while we're working at home:

Fully shut down your KPMG laptop at the end of each (this makes it harder for thieves to gain access), and lock it away securely. Don't allow anyone in your household to use it.

Log onto the KPMG network regularly in order to take automatic security updates containing patches that keep your device secure.

Ensure that KPMG and client documents can't be viewed by anyone in your household - keep them out of sight and put them away when you've finished working on them.

Don't dispose of any confidential KPMG or client documents through your normal household waste, unless it's been shredded first. You can use your own **cross-cut shredder**, as long as it's compliant with the DIN 66399 security level 4 standard, or higher.

If **highly confidential or sensitive information** may be discussed, consider moving to another room and shut the door, or sit as far away from others as possible.

Voice activated smart devices are always listening and may send sound recordings to their cloud-based servers. Try to avoid working near these devices or switch them off when on a call.

Change the name of your **default home Wi-Fi network** and your default **internet router password** (default passwords are available online to hackers). Use a strong password with numbers, letters and symbols.
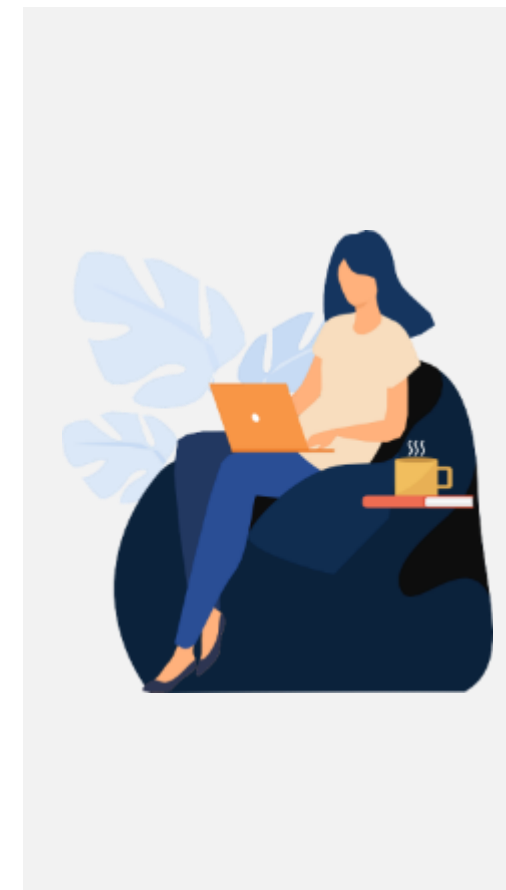
Work Securely on the Move

Be careful to avoid losing KPMG devices, documents or client information, or exposing it to the risk of being stolen when you're out of the office:

- Don't leave devices or documents (including notebooks and other meeting records) **unattended in a public place** at any time - always keep them with you.

- Never leave devices **unattended in a vehicle**, especially overnight.

- Always **fully shut down your laptop** before transporting it between locations. If it gets lost or stolen, it will be harder for an attacker to access if fully shut down.

- If your Member Firm provides **laptop privacy screens**, always use one to stop unauthorized people viewing information on your screen.

- Don't allow unauthorized people to **overhear you** discussing confidential information – move to a private area/room.

- Ensure you use a **secure VPN connection** if you need to use public Wi-Fi to access the internet from a KPMG laptop. Public Wi-Fi is unsecured, and may leave you exposed to attacks.

- Turn off the **Bluetooth** on your mobile device, unless needed, and don't accept uninitiated pairing requests from other devices – to prevent an attacker gaining access to your device.

> Before you travel internationally on business, understand that the information and devices in your possession could be at greater risk of loss, theft, or even espionage, with the resulting potential disclosure of information. If you believe that your destination poses a higher-than-normal risk, consider taking additional safeguards before you depart and during your travels. Minimize the amount of information you take with you and consider traveling with a 'clean' laptop.
>
> Keep your mobile device, laptop, tablet and any other equipment or documents with you whenever possible.

Work Securely at KPMG Premises

Security at KPMG premises is everyone's responsibility, so please help to maintain a safe and secure working environment.

Keep a secure workspace

Keeping **a clear and confidential workspace** (e.g. desk, meeting room, quiet room) helps to avoid information loss and theft, and gives clients and guests, the confidence that KPMG is safeguarding information appropriately.

Confidential meetings or conversations

- Avoid discussing **confidential or commercially sensitive information** openly (e.g. in an open-plan office or elevator.
- At the end of a meeting, make sure any **information on whiteboards** is erased, and **flip charts** or **notes** are taken with you or disposed of securely.

Documents

- Pick up any **print-outs** immediately.
- Dispose of unwanted confidential documents in a designated **secure disposal bin**.

Laptops

- Where possible, secure your laptop with a **cable lock**.
- Use a **privacy screen** (if issued) so information can't be read by passers-by.
- Never write down your **passwords**.

- Lock your **laptop screen** whenever you leave it unattended. Press "Ctrl_Alt_Del" and then "Enter" (or the Windows key and "L" key).
- When leaving your workspace for the day, take your laptop with you or make sure it's **locked** in a cabinet or secure location.

Keep your office – and colleagues – safe from intruders - If someone without an ID badge tries to enter the office as you're walking in or out (known as "tailgating"), **don't let them in.** Challenge them and escort them to reception if necessary. And when in KPMG premises, **always display your identification badge** to show that your access is authorized, and remove it when you leave.

© 2024 KPMG-Ukraine Ltd., a company incorporated under the Laws of Ukraine and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Document Classification: KPMG Public | 184

Scenario 7 –
Working Securely
With Clients

Scenario 7 – Working Securely With Clients

Gabriel and Eva have just won a new piece of client work, for a major healthcare provider.

They now have to ensure that they securely manage all of the risks in the project.

What can they do to ensure they work securely with the client?

Which of these should you do to work securely with clients?

Remove client data from client site without prior permission

Check client requirements on connecting to their network

Contact the NITSO if the client requires a policy exception

Follow relevant client as well as KPMG policies

Leave KPMG devices unattended at the client site

Only follow KPMG policies, not the client's

Which of these should you do to work securely with clients?

APPROPRIATE TO ACCES

Check client requirements on connecting to their network

Contact the NITSO if the client requires a policy exception

Follow relevant client as well as KPMG policies

INAPPROPRIATE TO ACCES

Remove client data from client site without prior permission

Leave KPMG devices unattended at the client site

Only follow KPMG policies, not the client's

Scenario 7 – Working Securely With Clients

The client requires the team to build an application that will house sensitive personal data on patients' medical conditions, in a cloud environment.

Gabriel has a lot of experience in this area, and wants to get started right away.

But he wonders whether due to the sensitivity of the data, the solution will need to undergo a risk assessment at some point?

At what point should Gabriel initiate a risk-assessment of the solution?

Scenario 7 – Working Securely With Clients

At what point should Gabriel initiate a risk-assessment of the solution?

A. He should do this after the solution has been built, so that the assessing team can investigate the full functionality of the tool.

B. He should initiate this process now, before he begins any work on the solution.

Scenario 7 – Working Securely With Clients

At what point should Gabriel initiate a risk-assessment of the solution?

A. He should do this after the solution has been built, so that the assessing team can investigate the full functionality of the tool.

B. He should initiate this process now, before he begins any work on the solution.

Scenario 7 – Working Securely With Clients

It's important to make sure **all** projects involving KPMG or client data are information and privacy risk-assessed as early as possible, as this enables the firm to analyze, identify and minimize the risks of a project or initiative before you start work on it, and to put in place the necessary security and privacy controls.

Precautions must also be taken to secure personal and sensitive personal data against loss or unauthorized disclosure. These should include appropriate technical, physical and organizational security measures according to the sensitivity of the information and the level of risk associated with the processing of it (e.g. protecting account access with strong password requirements and multi-factor authentication).

! Follow the risk-assessment process in your Member Firm (e.g. consult ITS or the NITSO) for all projects and initiatives where data or IT assets are involved, or where projects could introduce information or privacy risk.

Scenario 7 – Working Securely With Clients

Gabriel decides to contact the risk assessment team now, before he starts any work.

He wants to make sure that all the technical security requirements are built into the design from the outset.

A few weeks later, Gabriel and Eva are meeting the client at their office.

The client are showing them a set of data they plan to provide, but Eva notices that it contains more details about the patients than is necessary for the project's objective.

How should Eva respond to the client?

Scenario 7 – Working Securely With Clients

How should Eva respond to the client?

A. She should ask the client to redact the dataset to remove the unnecessary columns before they provide it.

B. She should accept the dataset with the extra columns, as this information may come in useful at a later stage of the project. Also, it may offend the clients if you question the data they're providing for their own project.

Scenario 7 – Working Securely With Clients

How should Eva respond to the client?

A. She should ask the client to redact the dataset to remove the unnecessary columns before they provide it. ✓

B. She should accept the dataset with the extra columns, as this information may come in useful at a later stage of the project. Also, it may offend the clients if you question the data they're providing for their own project.

Scenario 7 – Working Securely With Clients

If you are working with personal or sensitive personal data, it's important not to accept more information than is necessary for the purpose for which it was initially collected. This is part of KPMG's Data Privacy Principles that ensure we comply with data privacy law.

! If a client provides more information than is necessary for the purposes of your engagement, notify your engagement manager or leader who can speak to the client about this.

Scenario 7 – Working Securely With Clients

Eva thanks the client, but suggests that because of data privacy laws, it would be better to only take what is necessary to fulfil the terms of the engagement contract.

The client agree that this is the right course of action, and thank Eva for reminding them of the data privacy laws.

Scenario 7 – Working Securely With Clients

In this scenario you learned about managing engagement risks when working with clients, including:
- working securely on client site,
- following the information protection plan (IPP) for an engagement,
- ensuring that any necessary aspects of the engagement undergo a risk assessment at the start of the project, and
- complying with Data Privacy rules e.g. not taking more data than is needed from the client for the purpose of the engagement.

Select KEY CONSIDERATIONS to find out more.

Client Queries & Questionnaires

KPMG member firms are often asked by clients, prospective clients, vendors, regulators and other stakeholders about our **policies, procedures and controls** for safeguarding confidential information.

Typical questions and requests for information include

Does KPMG have **information security policies**?

How does KPMG **protect the data** we receive?

Does KPMG have **business continuity and disaster recovery plans**?

Do we share copies of our **policies**?

Does KPMG provide information protection and privacy **training**?

Is KPMG **ISO 27001 certified**?

May our clients **audit** our security and privacy controls, and/or perform a **penetration test** of our systems and network?

If you receive a client query or questionnaire

Contact your member firm **National IT Security Officer (NITSO)** as soon as possible.

They will serve as the focal point for responding to clients or other stakeholders about KPMG's information security practices.

Sensitive personal information

KPMG holds Personal Data about people, including employees, contractors, clients or employees of clients. We also handle and process large volumes of personal data on behalf of clients.

> Personal Data is any information about an individual that can be used on its own, or in conjunction with other information, to identify a natural living individual.

> Sensitive Personal Data may include Personal Data that reveals an individual's:

Examples:

- Name
- Address
- Date of birth
- Email address
- Phone number
- ID number
- Person's voice or image contained in audio/video recordings

Examples:

- Race or ethnicity
- Political opinions
- Religious or philosophical beliefs
- Criminal background
- Trade union memberships
- Health details
- Sexual orientation
- Biometric or genetic information

Sensitive Personal Data is likely to be of a private nature and **could be used in a discriminatory way**, so it needs to be treated with even more care than Personal Data. Explicit consent is generally required from individuals in order to process Sensitive Personal Data.

Working Securely on Client Sites

Protect KPMG devices and documents taken off-site to the same level as they would be on KPMG premises

- Never leave **KPMG devices (laptops and mobile phones)** unattended. Where possible, use a security cable lock (attached to a non-movable anchor point) to secure your laptop if you don't have access to lockable storage at the client site.

- **Lock your laptop screen** whenever you leave it unattended. Press "Ctrl_Alt_Del" and then "Enter" (or the Windows key and "L" key).

- If you're working on confidential information on your laptop, use a **privacy screen** (if available).

- If you leave laptop bags and other bags unattended, make sure they don't contain **any devices or sensitive KPMG or client information**.

- Don't leave **documents** unattended – where possible lock them away in a secure desk drawer or cabinet.

- Don't handle KPMG information **not relevant to the client engagement** when you're at client sites, unless this is absolutely necessary.

- Don't remove any **client provided documentation** or **removable electronic media** from the client site, without the client's permission and approval from the Engagement Manager.

- Dispose of all **confidential waste** into the Client's confidential waste bins.

- Be aware that you may need to adhere to **Client Information Security policies** as well as KPMG's.

Connecting to a client network

If you're working at a client site, you'll likely need to **access the client's network**, or to access KPMG systems through a client's internet connection. To maintain the security and integrity of KPMG's and the client's IT systems, consider this guidance *before* you connect:

Follow all relevant KPMG policies

Get **written permission** from the client and the engagement partner to access the client network. Contact your ITS department for help with any technical or security requirements.

(Although you don't typically need written permission to log onto **guest Wi-Fi**, you may have to sign an Acceptable Use statement).

Contact the client's IT department

Consult with the **client's IT department** to meet any security, technical or procedural requirements. If a client asks you to make changes to your KPMG-issued laptop computer or other equipment, contact your ITS department before doing so.

Follow client IT Security and Use policies

Comply with both **KPMG and client policies** related to the use of their network and systems. The client may not, for instance, permit the use of their resources for personal use. Similarly, they will likely not want their resources to be used for work related to other KPMG clients.

Don't assume that any two clients have the same requirements for connecting to their networks.

Any damage or data loss resulting from your failure to follow either KPMG or client policies could result in breaches of confidentiality, reputational damage, the loss of engagements or legal action against KPMG.

Client personnel connecting to KPMG networks

If a client needs to connect to the KPMG network in the course of collaborating with you, **submit a request** to your National IT Security Officer (NITSO). Once the NITSO has reviewed and approved the request, ensure that **appropriate procedures** are followed – including (where possible), ensuring that clients connect their devices via the guest Wi-Fi network.

Using Secure Cloud Services

Be wary of using **unauthorized public cloud services** to store or transmit information.

Popular services such as **Gmail, Dropbox, Siri, Google Translate and Generative AI tools** may be useful, but they aren't permitted (unless the local NITSO has pre-approved an exception) for processing, storing or sharing KPMG member firm or client information for several reasons.

The risks of using unauthorized Cloud services include

01 Confidential KPMG or member firm client information/data could be **leaked** to the public as a result of a service being compromised.

02 Data could **survive** on the service after you delete it, which in turn could breach our member firms' data retention policies

03 Data may be **stored** without proper segregation from the data of other users, allowing possible accidental or malicious disclosure to third-parties

04 Personal information may be **transferred** across borders, which could compromise the KPMG Privacy Policy or violate local laws

05 Employees of the to view and copy service may be able the data you upload

If a client requests the use of an **unauthorized Cloud service** to exchange files during the course of an engagement, the engagement partner should first consult with Quality & Risk Management.

Non-approved cloud services can be authorized by the **NITSO and the RMP** following a formal risk assessment.

Assessing Security and Privacy Risk in Projects

It's important to make sure all projects involving KPMG or client data are **information and privacy risk-assessed** as early as possible, as this enables the firm to analyze, identify and minimize the risks of a project or initiative before you start work on it.

It enables us to **understand the existing system or environment** by analyzing related information (e.g. applications, network architecture, business processes etc.), or to understand more about the **data being processed**.

Initiating this process at an **early stage of the project**, allows us to put in place the necessary security controls.

Follow the risk-assessment process in your Member Firm for all projects and initiatives where data or IT assets are involved, or where projects could introduce information risk. Such projects may include:

- **New IT systems and networks** that support business processes and data e.g. cloud investment decisions, generative AI

- **Material business changes** (e.g. merger, acquisition or divestment)

- **New business processes**

- **Business applications**

- **New KPMG premises**

- **Projects** involving the processing of **sensitive, personal data**

If you want to find out more about Information and Privacy risk- assessments, contact your local National IT Security Officer (NITSO) and/or Quality and Risk Management personnel.

Policy exception requests - If you receive one from a client during the course of an engagement – e.g. to use/install non-approved software onto KPMG devices – consult the engagement lead, who will review and assess the request in conjunction with the NITSO and Risk Management Partner (RMP).

Scenario 8 – Data Privacy Principles

Scenario 8 – Data Privacy Principles

Sohail is a manager working in the Corporate Tax team.

He's advising a client on employee rewards, and as this involves processing employee data, he wants to understand more about KPMG's Data Privacy principles

10 Data Privacy Principles

1 **Transparency** - KPMG Firms will provide individuals with information about how we process their Personal Information, to the extent necessary to ensure that processing is fair.

2 **Purpose Limitation** – KPMG Firms will only process Personal Information for the purposes:

set out in any notice made available to the relevant individuals which are relevant to KPMG,
as required by law or,
where consented to by the relevant individuals.

3 **Data Quality & Proportionality** - Personal Data should be kept accurate and where necessary, up to date. The Personal Information KPMG Firms hold must be adequate, relevant and not excessive for the purposes for which they are transferred between the KPMG Firms, and should only be retained for as long as necessary for the purposes of the relevant processing.

4 **Security and Confidentiality** - Reasonable precautions must be taken to secure Personal Data against accidental or unlawful destruction or loss, alteration, unauthorized disclosure or access. Additional measures may be necessary so as to respect local customs, laws or regulations.

5 **Access, Rectification, Deletion and Objection** – Individuals should have access to their Personal Data, where those requests are reasonable and permitted by law. An individual may object to processing if there are compelling legitimate grounds and KPMG will rectify, amend, or delete Personal Data as appropriate.

10 Data Privacy Principles

6 **Sensitive Data** - Where KPMG Firms process Sensitive Personal Data, they will take such additional measures (e.g. relating to security) as are necessary to protect such Sensitive Personal Data, in accordance with applicable law.

7 **Data Used for Marketing Purposes** - Where KPMG Firms process Personal Information for the purposes of direct marketing, those KPMG Firms will have effective procedures allowing individuals at any time to "opt-out" from having their Personal Information used for such purposes.

8 **Automated Processing** - Where KPMG Firms process Personal Information on a purely automated basis that has a significant impact on an individual, those KPMG Firms shall give the individual the opportunity to discuss the output of such processing before making those decisions (save to the extent otherwise permitted under applicable law).

9 **Data Minimization** - Where KPMG Firms retain an individual's personal information, those KPMG Firms will do so in a form identifying or rendering an individual identifiable only for so long as it serves the purpose(s) for which it was initially collected or subsequently authorized except to the extent permitted by applicable law.

10 **Information Transfer and Compliance** – Within the global network of KPMG Firms, Personal Data may be transferred outside the country which it was collected for legitimate business activities in accordance with applicable law.

Scenario 8 – Data Privacy Principles

One day, he receives an email from an employee of his client.

They are unhappy that KPMG are handling personal information about them in the course of the engagement, and would like to know more information about this.

What should Sohail do about this complaint?

Scenario 8 – Data Privacy Principles

What should Sohail do about this complaint?

A. He should inform his engagement leader immediately so it can be dealt with promptly.

B. He should inform the client immediately. It's their employee so they need to deal with this complaint, not KPMG.

Scenario 8 – Data Privacy Principles

What should Sohail do about this complaint?

A. He should inform his engagement leader immediately so it can be dealt with promptly.

B. He should inform the client immediately. It's their employee so they need to deal with this complaint, not KPMG.

Scenario 8 – Data Privacy Principles

That way, the engagement leader can contact the local Privacy Liaison who will be able to advise on the appropriate next steps.

! We have an obligation to deal with these types of inquiry, when we are processing an individual's personal data as part of an engagement.

Scenario 8 – Data Privacy Principles

Sohail decides to inform his engagement leader immediately about the complaint, as KPMG have an obligation to respond to these types of inquiry within a certain timeframe.

Later, Sohail receives another email – this time from a supplier notifying him that they will be moving their cloud data storage location from Germany to Chile.

He realises that this will have an impact on his engagement, as personal data is being stored in this cloud solution.

What should Sohail do next?

Scenario 8 – Data Privacy Principles

What should Sohail do next?

A.He should tell the supplier to go ahead, as the service that the supplier provides is vital to the processing of data on this engagement, so it must continue uninterrupted.

A.He should consult with the Privacy Liaison to determine if this change will meet any applicable regulatory data privacy requirements, and additional privacy requirements (if any) agreed with the client in the engagement terms.

Scenario 8 – Data Privacy Principles

What should Sohail do next?

A.He should tell the supplier to go ahead, as the service that the supplier provides is vital to the processing of data on this engagement, so it must continue uninterrupted.

A.He should consult with the Privacy Liaison to determine if this change will meet any applicable regulatory data privacy requirements, and additional privacy requirements (if any) agreed with the client in the engagement terms. ✓

Scenario 8 – Data Privacy Principles

Moving personal data processing to a different country (including outside of the European Economic Area (EEA)) may trigger additional data privacy requirements for KPMG to be compliant.

Sohail should consult with the Privacy Liaison so KPMG understands the implications of moving the data, which may include a transfer impact assessment.

! When in doubt, speak to your local Privacy Liaison for additional guidance on International Data Transfers, including transfers between Member Firms.

Scenario 8 – Data Privacy Principles

Before replying to the supplier, Sohail immediately consults with the Privacy Liaison, so KPMG will understand the implications of moving the data (which may include a transfer impact assessment
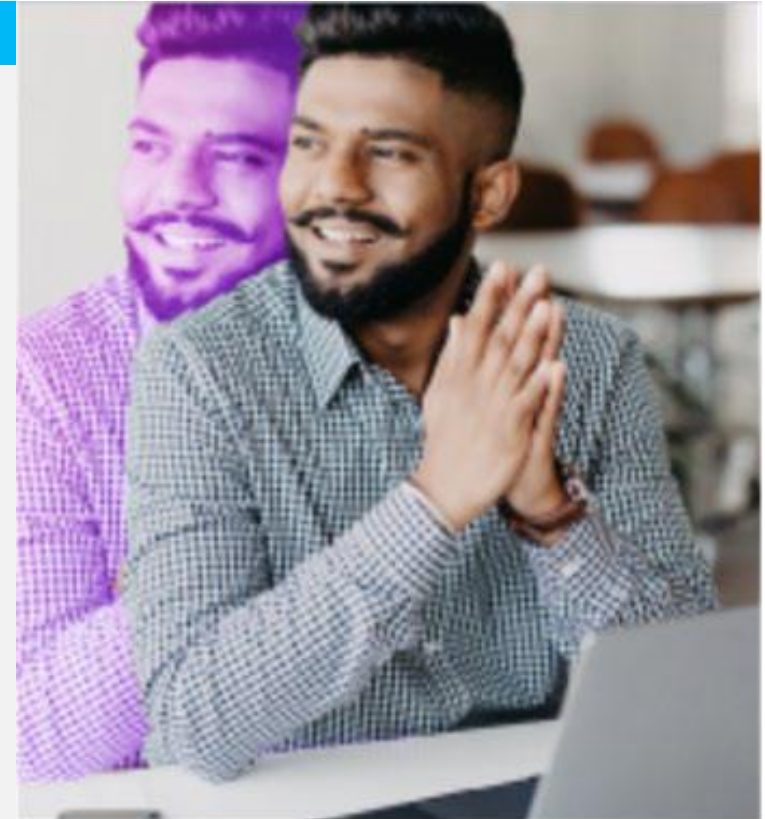
Scenario 8 – Data Privacy Principles

In this scenario you learned about:
- Data Privacy principles,
-complaints from individuals regarding KPMG's handling of their private data, and
-considerations around international data transfers.

Select KEY CONSIDERATIONS to find out more.

Data Privacy Principles

KPMG follows 10 Data Privacy Principles to help us comply with data privacy law

These principles apply to **everyone at KPMG** who has access to personal information, including you.

These principles are **shared and followed** by all KPMG member firms.

The Data Privacy Principles provide **a common foundation** to help us to better serve our clients, our colleagues, and our communities.

You can find more information on the Data Privacy principles in the **Global Privacy Policy** (under Resources).

1. Transparency
2. Purpose Limitation
3. Data Quality & Proportionality
4. Security and Confidentiality
5. Access, Rectification, Deletion and Objection
6. Sensitive Data
7. Data Used for Marketing Purposes
8. Automated Processing
9. Data Minimization
10. Information Transfer and Compliance

Data Controller v Data Processor

One feature of data privacy legislation is the different roles of Data Controllers and Data Processors

Both must comply with privacy laws, but their responsibilities are different:

Data Controllers decide for what purpose and how the personal data is processed.

Data Processors process the personal data on behalf of the Data Controller.

For **KPMG data**, KPMG acts as a Controller and follows the 10 Data Privacy Principles.

For **client data**, our contract will specify whether KPMG is acting as a Data Controller or Data Processor.

Processing means any operation or set of operations which is performed on personal data or on sets of personal data - whether or not by automated means, such as:
- collection
- recording
- organisation
- structuring
- storage
- adaptation or alteration
- retrieval
- consultation
- use
- disclosure by transmission
- dissemination or otherwise making available
- alignment or combination
- restriction
- erasure or destruction

Data Subject Access Requests (DSARs)

A Data Subject Access Request (DSAR) is a request by an individual for access to information about personal data KPMG is processing about them

This allows individuals to **verify the lawfulness** of the processing.

KPMG **must reply to DSARs in a timely manner** or there may be problems with our regulators.

If you receive a DSAR, **report it using your local processes** for DSAR intake or if you are not sure, contact your Privacy Liaison for help.

The team that handles DSARs will **review it**, work with any stakeholders required for the response, and escalate as needed.

International Data Transfers

Within the global network of KPMG Firms

- Personal Data **may be transferred** outside the country in which it was collected - including countries outside of the EEA - for legitimate business activities in accordance with applicable law.

- In accordance with applicable law, KPMG Firms **may store Personal Data** in facilities operated by other KPMG Firms and/or third parties on behalf of the KPMG Firms outside the country in which the data was collected.

- Personal Data **must not be transferred** to another country unless the transferor has assurance that an adequate level of protection is in place in relation to that Personal Data as required under applicable law.

- In the case of each KPMG Firm, an adequate level of protection is created by the **Inter-Firm Data Transfer Agreement**, which each KPMG Firm shall abide by.

To third parties outside of the KPMG network

- KPMG Firms will ensure that where personal information is **transferred to third parties outside of the KPMG network** for processing (for example to KPMG's service providers to support KPMG's business), that this is only done where the personal information is adequately protected.

- KPMG Firms will achieve this by entering into **written agreements** with third parties which impose obligations that reflect the requirements of this policy.

Concerns

If you have an engagement concern about an international data transfer, let the engagement partner know and for general concerns, consult your **Privacy Liaison**.

KPMG Confidential

Conclusion

Conclusion

You have reached the end of the course, and should now be able to:

- Understand key threats to KPMG and its personnel

- Understand how to make appropriate choices in following KPMG information protection and data privacy policies

- Know how to protect confidential information, (including KPMG and client information) in all locations where KPMG personnel work or might discuss work

- Understand the financial, legal and regulatory, and reputational impact to KPMG's business, clients, and personnel of failing to secure confidential information

- Understand what Personal Data is and why it is important to protect Personal Data

- Understand KPMG's 10 Data Privacy Principles and how to apply them as a Data Controller or Data Processor

- Know the key best practices for protecting Personal Data

- Know the different mechanisms for international transfers of Personal Data

- Understand who to contact and appropriate next steps when you become aware of a possible or actual information security or data loss incident

If you need to report a Security Incident

A security incident is 'any event that may compromise the confidentiality, privacy, integrity, or availability of our information or information systems'. It doesn't have to be something that you know has happened - just something that causes you concern that our information may be threatened. It could be:

- The loss of any portable device (such as a laptop, mobile phone, tablet or storage drive), or documents
- A data breach due to unauthorized network access
- A malware threat from selecting an email link or attachment
- Your login credentials may have been revealed to someone else
- If you've mistakenly sent a confidential email to the wrong person, or misdirected confidential information via other means
- Unauthorized visitors on KPMG premises
- If you know or suspect that information security procedures in projects or engagements have not been followed correctly
- If you suspect that an unauthorized person has seen or overheard confidential information being discussed
- Use of unauthorized email or file-sharing tools
- Installation of non-approved or unlicensed software (check with your Member Firm ITS)

Report actual or suspected security incidents immediately, so that the appropriate corrective actions can be quickly taken. Follow the reporting procedure in your Member Firm e.g. contact the IT Service Desk or the local Risk Management team.

If it's a client-related incident, get advice from your local Risk Management team first. Don't discuss with the client until an appropriate KPMG response has been agreed.

Document Classifica

Further information and contacts

General queries

If you have any queries on **this course or its contents**, you can contact the

Global Information Protection Training and Awareness team, and the Global Data Privacy team.

Visit the portal pages here:

Global Information Protection Training and Awareness portal
Global Data Privacy portal

Local contacts

If you have any questions about local Information Protection or Data Privacy
policies, please contact
- National IT Security Officer (NITSO) (for Ukraine)
- ua-sgua-fmethicsandindependence@kpmg.ua (Quality & Risk Management team)
- ua-fmkieihl@kpmg.ua (Data Privacy team)

The course is now complete.
Thank you

KPMG

kpmg.ua