Compliance e-learning & explainer scripts

30 practice scripts from VO Journey Academy. Free to record, free to use in your reel. Download the PDF to mark up in the booth, or print it straight from here.

Why Privacy Rules Exist

Data privacy, module introduction · Adult (30-45) · Neutral American · 90 seconds

[On screen: Protecting Personal Information - Annual training]

Think about everything a company might know about you. Your home address. Your date of birth. Your bank details. Maybe your medical history, or the names of your children.

Now imagine all of that turning up in a stranger's inbox because someone clicked the wrong name in an email.

Every record in our systems belongs to someone like that. A real person who trusted us with it.

That's why privacy rules exist. Not to slow you down, but to make sure the information people give us is used only for the reason they gave it, kept only as long as we need it, and protected while we have it.

[On screen: What this course covers]

In this course, you'll learn what counts as personal data, how to handle it day to day, and what to do if something goes wrong.

It takes about twenty minutes. There's a short quiz at the end, and you'll need to score eighty percent to complete it.

[On screen: Who this applies to]

This training applies to everyone at Brightwater Health Systems, including contractors and temporary staff. It doesn't matter whether you work with patient records all day or

only see a customer's name once a month. The rules are the same.

Let's start with a simple question. What exactly is personal data?

What Counts as Personal Data

Data privacy, definitions · Adult (25-40) · Neutral American · 2 minutes

[On screen: What counts as personal data?]

Personal data is any information that relates to an identifiable person. That second word, identifiable, is doing a lot of work.

Some examples are obvious. A name. A home address. A phone number. An email address. A Social Security number.

Others are less obvious. An employee ID number. A photo of someone's face. A car's license plate. The location data from a phone. Even an IP address can count.

[On screen: Combinations matter]

And sometimes, pieces of information that seem harmless on their own become personal data when you put them together. A job title, a department, and a start date might point to exactly one person in a small office.

So a good rule of thumb is this: if the information could help someone work out who a person is, treat it as personal data.

[On screen: Sensitive personal data]

Some personal data is more sensitive, and needs extra care. This includes health information, racial or ethnic background, religious beliefs, sexual orientation, union membership, and biometric data like fingerprints.

If this kind of information is lost or misused, the harm to the person can be serious, from discrimination to identity theft. So access is tighter, and the rules for sharing it are stricter.

[On screen: Where you'll find it]

Where will you come across personal data at work? Probably more places than you'd think. Customer databases, yes. But also spreadsheets on shared drives, email attachments, printed forms, call recordings, and screenshots in support tickets.

[On screen: Quick check]

Let's try a quick one. A spreadsheet lists order numbers and delivery postcodes, but no names. Is that personal data?

In many cases, yes. Combined with order history, a postcode can point to a single household.

In the next section, we'll look at how to handle personal data safely, from the moment you receive it to the moment it's deleted.

The Misdirected Email

Data privacy, incident response scenario · Adult (25-40) · Neutral American · 90 seconds

[On screen: Scenario - 4:52 on a Friday]

It's 4:52 on a Friday. You're sending a spreadsheet of employee salary changes to Chris in Finance.

You type "Chris," the address fills in, you hit send, and you're reaching for your coat when you notice it.

It went to the wrong Chris. Chris from an outside vendor.

What now?

[On screen: Step 1 - Don't wait]

First, don't wait until Monday. And don't try to quietly fix it yourself. Report it right away. A privacy incident needs attention within hours, not days, because some incidents must be reported to regulators within a strict deadline.

[On screen: Step 2 - Report it]

Use the Report an Incident button on the intranet homepage, or call the privacy team directly. Tell them what was sent, who it went to, and when.

[On screen: Step 3 - Recall and request]

Try to recall the message if your email allows it. The privacy team may also ask you to contact the recipient and request that they delete it and confirm in writing.

[On screen: Step 4 - Don't forward or delete evidence]

Don't delete your sent message. The team may need it to understand what happened.

Mistakes like this happen to careful people. What matters most is how quickly they're reported. Nobody will be in trouble for reporting a mistake promptly. Hiding one is a different matter.

Clean Desk, Locked Screen

Security awareness, physical security · Young adult (18-25) · Neutral American · 60 seconds

[On screen: Clean desk, locked screen]

Two habits. Ten seconds each. Big difference.

[On screen: Lock your screen]

First, lock your screen every time you step away. Coffee, meeting, bathroom, doesn't matter. It takes one keyboard shortcut, and it's on the screen now.

An unlocked laptop is an open door to your email, your files, and every system you're signed in to. Anyone walking past can use it, and whatever they do will look like it was you.

[On screen: Clear your desk]

Second, clear your desk at the end of the day. Printed reports, sticky notes with passwords, customer forms. Put them in a locked drawer or the secure shred bin.

Cleaners, visitors, and contractors pass through our offices every day. Most of them are perfectly trustworthy. But you don't need to find out.

Lock it. Clear it. Every time.

Spotting a Phishing Message

Security awareness, phishing · Adult (30-45) · Neutral American · 2 minutes

[On screen: Spotting a phishing message]

Most cyberattacks don't start with a clever hacker breaking through a firewall. They start with an email that someone opens and trusts.

That's called phishing. Here's an example.

[On screen: Sample email]

"From: IT Service Desk. Subject: Action required, your mailbox is almost full. Your mailbox has reached ninety-eight percent of its storage limit. To avoid losing incoming messages, verify your account within twenty-four hours using the link below."

Looks routine, doesn't it? Let's look closer.

[On screen: Sign 1 - The sender address]

First, the sender. The display name says IT Service Desk, but the actual address is itservice at mail-verify-center dot net. Our IT team would only ever email you from our own company domain.

[On screen: Sign 2 - Urgency]

Second, the urgency. Twenty-four hours, or you'll lose messages. Pressure is a classic tactic. It's meant to make you act before you think.

[On screen: Sign 3 - The link]

Third, the link. If you hover over it without clicking, you'll see it goes to a site that has

nothing to do with us.

[On screen: Sign 4 - The request]

And fourth, what it's asking for. Any message that asks you to sign in through a link, share a password, or approve a login you didn't start should make you stop.

[On screen: What to do]

So what should you do if you get a message like this? Don't click the link, don't reply, and don't forward it to colleagues to ask what they think. Use the Report Phish button in your email toolbar. It sends the message to our security team and removes it from your inbox.

And if you already clicked? Report it anyway, right away, and tell the security team what you entered. Acting quickly can stop a small mistake from becoming a serious breach.

Next, you'll look at five messages and decide which ones are safe.

Phishing Knowledge Check

Security awareness, knowledge check · Adult (25-40) · Neutral American · 60 seconds

[On screen: Question 3 of 5]

You receive a text message that appears to come from your manager. It says: "In a client meeting, can't talk. Need you to buy four gift cards for a customer thank-you. I'll reimburse you today. Send me the codes."

What should you do?

A. Buy the gift cards quickly, since your manager is busy.
B. Reply to the text and ask for more details.
C. Contact your manager using a phone number or chat you already know is theirs.
D. Forward the text to your team to see if anyone else got it.

[On screen: Learner selects B]

Not quite. Replying to the text keeps you talking to whoever sent it, and scammers are good at having an answer ready.

[On screen: Learner selects C]

That's right. Always verify an unusual request through a separate channel you already trust. Requests for gift cards, wire transfers, or urgent secrecy are common signs of a scam, even when the name looks familiar.

The Caller Who Knew Too Much

Security awareness, social engineering role-play · Adult (30-45) · Neutral American · 2 minutes

Cast: AGENT CALLER

On screen: Listen to this call. Notice the techniques the caller uses.

AGENT Service desk, this is Tamsin. How can I help?

CALLER Hi Tamsin, it's Greg Holloway from the Denver office. I'm really hoping you can save my afternoon here.

AGENT I'll do my best. What's going on?

CALLER So I'm locked out of my account, and I'm presenting to the regional directors in, like, fifteen minutes. My badge number's 40318, I'm in sales, my manager's Lena Park. Can you just reset my password and read me the temporary one?

AGENT I'm sorry you're in a rush. I can definitely help you reset it. I'll just need to send a verification code to the mobile number on your account.

CALLER Yeah, see, that's the problem. I left my phone in the car, and I'm on a conference line right now. Can we skip that part, just this once?

AGENT I understand. Unfortunately, I can't skip verification. It protects your account as much as anyone's.

CALLER Tamsin, I'm serious, my boss is going to kill me if I'm not on this call. You've got my badge number, my manager's name. What else do you need?

AGENT I hear you, and I'm sorry about the timing. What I can do is send the code to your phone, and you can grab it from the car. Or your manager can call us from her own line to confirm it's you.

CALLER Forget it. I'll figure something else out.

AGENT Okay. Good luck with the presentation, Greg.

On screen: Pause and reflect

On screen: Name-dropping. Urgency. Details that are easy to find. A request to skip one step.

Did you notice how much the caller knew? Badge numbers and manager names can often be found online or overheard. Knowing details isn't proof of identity. That's why verification steps are never skipped, no matter how convincing the story.

Passwords and Passphrases

Security awareness, credentials · Adult (40-55) · Neutral American · 60 seconds

[On screen: Strong passwords]

Short, complicated passwords are hard for you to remember and, surprisingly, not that hard for a computer to guess.

Long passwords are much stronger. And the easiest way to make one long is to use a passphrase.

[On screen: Four random words]

Pick four or more random words that don't belong together. Something like: purple, ladder, biscuit, harbor. Picture it. A purple ladder, covered in biscuits, down at the harbor. You'll remember it tomorrow. An attacker's software will struggle with it for years.

[On screen: One account, one password]

The other rule is just as important. Never reuse a password. If one site is breached, criminals try the same password everywhere else.

That's what the company password manager is for. It creates and remembers strong passwords for every account, so you only need to remember one good passphrase.

And turn on multi-factor sign-in wherever you can. It's the single best thing you can do.

Respect at Work: Course Introduction

Harassment prevention, course introduction · Adult (40-55) · Neutral American · 60 seconds

[On screen: Respect at Work - Annual training]

Everyone deserves to come to work and feel safe, respected, and able to do their job.

Most of the time, that's exactly what happens here. But harassment still occurs in workplaces everywhere, including good ones, and it's often not reported.

This course is here to change that.

[On screen: What you'll learn]

Over the next thirty minutes, you'll learn what harassment is and what it can look like, including some forms that are easy to miss. You'll learn how to respond if you experience it or see it happen. And you'll learn how to report a concern, and what happens after you do.

Some of the scenarios in this course may be uncomfortable. If anything brings up something personal for you, you can pause at any time. Support is available through our employee assistance program, and the details are on screen now.

Let's begin.

What Harassment Looks Like

Harassment prevention, definitions · Adult (30-45) · Neutral American · 3 minutes

[On screen: What harassment looks like]

Harassment is unwelcome conduct related to a personal characteristic, such as a person's sex, race, religion, age, disability, sexual orientation, or gender identity, that

makes someone's work environment hostile, intimidating, or offensive.

That's the formal definition. Let's look at what it means in practice.

[On screen: Verbal]

Harassment can be verbal. Slurs. Jokes that target a group. Repeated comments about someone's body, clothing, or appearance. Questions about someone's private life that keep coming after they've made clear they don't want to answer.

[On screen: Non-verbal and visual]

It can be non-verbal or visual. Staring, gestures, or sharing images, memes, or videos that demean a group. This includes content shared in group chats and on personal social media, if it involves colleagues.

[On screen: Physical]

It can be physical. Unwanted touching, blocking someone's path, or standing too close after being asked to step back.

[On screen: Sexual harassment]

Sexual harassment is one specific form. It includes unwelcome sexual advances, requests for dates after someone has said no, and sexual comments or content. It also includes any situation where job benefits, like a promotion or a good shift, are linked to accepting sexual attention. That is always serious, even if it only happens once.

[On screen: Impact matters more than intent]

Now, an important point. Impact matters more than intent.

Someone may say, "I was only joking," or "I didn't mean anything by it." That may be true. But if the behavior is unwelcome and it's related to a personal characteristic, it can still be harassment. What matters is how it affects the person on the receiving end, and whether a reasonable person in their position would find it hostile or offensive.

[On screen: It doesn't have to be your manager]

Harassment can come from anyone: a manager, a coworker, a customer, a vendor, or a contractor. And it can happen anywhere work happens. That includes the office, a client site, a video call, a team dinner, or a message sent at midnight.

[On screen: Patterns]

Sometimes it isn't one big incident. It's a pattern of smaller ones. A comment in a meeting, then another in the hallway, then another in a chat. Each one might seem minor on its own. Together, they can make someone dread coming to work.

[On screen: What harassment is not]

It's also worth being clear about what harassment is not. A manager giving honest feedback about performance, assigning work, or holding someone to a deadline is not harassment, as long as it's done respectfully and consistently. Disagreement isn't harassment either.

[On screen: Knowledge check coming up]

In the next section, you'll read six short situations. For each one, decide whether it could be harassment, and what a good response would be. Some are clear. Some are not, and that's intentional.

The Bystander Moment

Harassment prevention, bystander intervention · Adult (25-40) · Neutral American · 90 seconds

[On screen: When you see it happen]

You're in the break room. A coworker makes a comment about a new team member's accent. A couple of people laugh. The new team member goes quiet and leaves.

You felt uncomfortable. But you didn't say anything. Most people don't. Not because they don't care, but because they don't know what to say in the moment.

So here are some options. You don't have to use all of them. Just one is enough.

[On screen: Direct]

Be direct, if you feel safe doing it. "That's not okay." Short and calm is often the most effective.

[On screen: Distract]

Distract. Change the subject, or give the person a reason to leave. "Hey, Mina, can you help me with something at my desk?"

[On screen: Delegate]

Delegate. Tell a manager or HR what you saw. You don't need to handle it alone.

[On screen: Follow up]

And follow up afterwards. Check in with the person it happened to. "I heard what he said. Are you okay?" That simple question can mean a great deal.

You won't always get it perfect. That's all right. Doing something, even something small and a little clumsy, is almost always better than doing nothing.

Reporting a Concern

Harassment prevention, reporting process · Adult (40-55) · Neutral American · 90 seconds

[On screen: How to report a concern]

If you experience harassment, or see it happen to someone else, you have several ways to report it. Choose the one that feels right to you.

[On screen: Option 1 - Your manager]

You can talk to your manager. If your concern involves your manager, you can go to any other manager you trust.

[On screen: Option 2 - People Team]

You can contact the People Team directly, by email, phone, or in person.

[On screen: Option 3 - The Candor Line]

Or you can use the Candor Line. It's run by an independent service, it's available twenty-four hours a day by phone or online, and you can choose to stay anonymous.

[On screen: What happens next]

When a concern is reported, it's reviewed promptly. If an investigation is needed, it's handled by trained people, and information is shared only with those who need to know.

You may not learn every detail of the outcome, for privacy reasons. But you will be told when the matter is closed.

[On screen: No retaliation]

And most importantly, no one will face any negative consequences for raising a concern in good faith. Not for reporting, and not for taking part in an investigation. That's a firm rule, and it's taken as seriously as the harassment itself.

Scenario: The Group Chat

Harassment prevention, branching scenario · Adult (25-40) · Neutral American · 2 minutes

[On screen: Scenario - The team chat]

You're part of an informal group chat with six people from your team. It started as a place to share lunch plans and complain about the coffee machine.

Lately, one member, Evan, has been posting memes that make fun of Tomas, the newest person on the team, who isn't in the chat. The memes mock his weight. A few people reply with laughing faces. Others say nothing.

Today, Evan posts another one.

What do you do?

[On screen: Choose one]

Option A. Ignore it. It's a private chat, and Tomas will never see it.

Option B. Reply in the chat. "Come on, this isn't cool. Can we stop?"

Option C. Say nothing in the chat, but report it to your manager or the People Team.

[On screen: Learner selects A]

You scroll past. Over the next few weeks, the memes keep coming. Eventually someone shows Tomas a screenshot. He feels humiliated, and he starts to wonder who on the team he can trust.

Private chats aren't really private, and harassment doesn't need the target to be present. Staying silent can look like agreement.

[On screen: Learner selects B]

Evan replies, "Relax, it's a joke." But two other people add, "Yeah, let's drop it." The posts stop.

Speaking up in the moment can work, especially when others back you up. If the behavior continues, it's still a good idea to report it.

[On screen: Learner selects C]

Your manager speaks with Evan and the group. The posts stop, and Evan is reminded of the standards that apply to all work communications, including informal chats.

Reporting is always an option, and it's especially useful if you don't feel comfortable challenging someone directly.

[On screen: Key point]

Both B and C are good responses. What matters is that the behavior doesn't go unchallenged.

Retaliation Is Its Own Violation

Harassment prevention, retaliation · Adult (30-45) · Neutral American · 60 seconds

[On screen: Retaliation]

When someone raises a concern, they're taking a risk. Our job is to make sure that risk never becomes a punishment.

Retaliation means treating someone badly because they reported a concern, or helped with an investigation. It's prohibited, and it's treated as seriously as the original misconduct.

[On screen: Examples]

It isn't always obvious. Leaving someone off meetings they used to attend. That is retaliation. Suddenly giving them the worst shifts. That is retaliation. Spreading rumors about why they complained, or pressuring them to drop it. That is retaliation too.

If you're a manager, be especially careful. Decisions about someone who has raised a concern should be based on clear, documented, job-related reasons, and it's wise to talk to the People Team first.

If you think you're experiencing retaliation, report it through any of the usual channels.

Our Code of Conduct in Plain Words

Ethics, code of conduct · Mature (55+) · Neutral American · 90 seconds

[On screen: The Ashgrove Code of Conduct]

Our Code of Conduct runs to thirty-two pages. You should read it, and you will need to confirm that you have.

But if you boil it down, it asks you to do four things.

[On screen: Be honest]

Be honest. In your reports, your expense claims, your conversations with customers, and your dealings with each other. If you're not sure something's true, say so.

[On screen: Be fair]

Be fair. Treat colleagues, customers, and suppliers with respect, and make decisions based on merit, not favors or friendships.

[On screen: Protect what's entrusted to us]

Protect what's entrusted to us. That includes company property, confidential information, and the personal data of the people we serve.

[On screen: Speak up]

And speak up. If something doesn't feel right, raise it. You don't need proof. A concern raised early is almost always easier to fix.

When you're not sure what to do, try a simple test. Would you be comfortable if your decision were explained on the front page of the local paper? Would you be comfortable

explaining it to someone you respect?

If the answer is no, pause, and ask for guidance. That's exactly what the Code is for, and it's why the Ethics Office is only a phone call away.

Conflicts of Interest

Ethics, conflicts of interest · Adult (40-55) · Neutral American · 2 minutes

[On screen: Conflicts of interest]

A conflict of interest happens when your personal interests could influence, or look like they influence, the decisions you make at work.

Notice the phrase "look like." A conflict doesn't mean you've done anything wrong. It means there's a risk that others might wonder whether you acted fairly.

Here are some common situations.

[On screen: Family and friends]

Family and friends. Your sister runs a catering company, and you're choosing a caterer for the annual conference. Even if hers is genuinely the best option, you shouldn't be the one making that decision.

[On screen: Outside work]

Outside work. You're offered a paid role advising a small company that sells software to businesses like ours. That could affect your judgment, and it may use knowledge you gained here.

[On screen: Investments]

Investments. You own a significant number of shares in a supplier you manage.

[On screen: Relationships at work]

Relationships at work. You're in a romantic relationship with someone you manage, or whose pay or promotion you influence.

[On screen: Having a conflict isn't wrong. Hiding one is.]

In every one of these cases, the answer is the same. Disclose it.

Having a conflict isn't wrong. Hiding one is.

To disclose, complete the short form in the Ethics section of the intranet. Your manager and the Ethics Office will review it, and in most cases, the fix is simple. Someone else makes the decision, or you step back from one part of a project.

[On screen: Keep it current]

Conflicts can change over time, so update your disclosure if your situation changes. And when in doubt, disclose. A two-minute form now can save you a very uncomfortable conversation later. It's always easier to explain something you reported than something someone else discovered.

Gifts and Hospitality

Anti-bribery, gifts and entertainment · Adult (30-45) · Neutral British · 90 seconds

[On screen: Gifts and hospitality]

Gifts and hospitality are a normal part of business. A box of biscuits at Christmas, a working lunch with a supplier, a branded notebook at a conference. None of that is a problem.

The problem comes when a gift is generous enough, or timed so conveniently, that it might influence a decision. Or look as though it could.

[On screen: The rules]

So here are our rules.

Gifts or hospitality worth less than fifty pounds are generally fine, as long as they're occasional and not cash.

Anything worth fifty pounds or more must be logged in the Gifts Register before you accept it, and approved by your line manager.

[On screen: Never acceptable]

Some things are never acceptable, whatever the value. Cash or anything like cash, such as vouchers or gift cards. Anything offered while a tender or contract negotiation is under way. And anything you'd feel awkward telling your manager about.

[On screen: Offering gifts]

The same principles apply when we're the ones offering. And be especially careful with public officials. Even modest hospitality to an official can raise serious concerns, so

always check with the Compliance team first.

If you're unsure, a polite "thank you, but our policy doesn't allow me to accept this" is always an acceptable answer.

The Facilitation Payment

Anti-bribery, branching scenario · Adult (40-55) · Neutral British · 2 minutes

[On screen: Scenario - A delayed shipment]

Nadia manages logistics for Fairhaven Engineering. A shipment of replacement parts for a customer's water treatment plant is being held at a port overseas.

The paperwork is complete. But a customs officer tells Nadia's local agent that the shipment could be "processed faster" if a small fee of about eighty pounds is paid in cash. There's no receipt, and there's no official fee schedule that mentions it.

The customer's plant is running on backup equipment. Every day of delay is a problem.

What should Nadia do?

[On screen: Three options]

Option one. Pay it. It's a small amount, it's common practice locally, and the customer needs those parts.

Option two. Tell the agent to pay it and include it in their invoice as a handling charge.

Option three. Refuse the payment, and escalate to the Compliance team and her manager straight away.

[On screen: Answer]

The right answer is option three.

A payment like this is known as a facilitation payment: a small, unofficial payment to speed up a routine government action. Many people assume small payments like this are harmless. But under our policy, and under the laws of many countries including the UK, they're treated as bribes.

Are facilitation payments ever allowed at Fairhaven? No. Not even small ones.

Option two is worse than option one. Disguising the payment in an agent's invoice doesn't make it acceptable. It adds false records on top of the bribe.

[On screen: The one exception]

There's one exception. If someone is facing a genuine threat to their safety or liberty, they may pay to stay safe. Safety comes first. But it must be reported to Compliance as soon as possible afterwards.

[On screen: What happens next]

In this case, Compliance works with the customer and the port authority through official channels. The shipment is delayed by three more days. That's frustrating. But it's the right call, and the customer is kept informed throughout.

Working with Third Parties

Anti-bribery, third-party due diligence · Adult (40-55) · Neutral American · 3 minutes

[On screen: Working with third parties]

Much of our work overseas happens through third parties. Sales agents, distributors, customs brokers, consultants, and joint venture partners.

These relationships are valuable. They're also where a large share of bribery risk sits.

Why? Because if a third party pays a bribe while acting on our behalf, the company can be held responsible, even if nobody here knew about it.

That's why we don't just check who we're hiring. We check how they work.

[On screen: Before we engage]

Before we engage a new third party in a higher-risk role, we carry out due diligence. That means finding out who owns and controls the business, whether they or their owners have links to government officials, whether they have the experience and staff to do the job, and whether there are any past allegations of corruption.

This is done through the Partner Review process on the Compliance portal. It usually takes two to three weeks, so build that into your plans.

[On screen: Red flags]

During that process, and throughout the relationship, watch for red flags. Here are some of the most common.

The partner asks to be paid in cash, or into an account in a different country from where they operate.

Their fee is unusually high for the work, or they ask for a large success fee tied to winning a government contract.

They're reluctant to explain what their services involve, or they refuse to sign our anti-bribery terms.

They were recommended by a government official, or a relative of one.

Or they say something like, "Don't worry about the details. I know how things work

here."

[On screen: A red flag isn't a verdict]

A red flag doesn't automatically mean something is wrong. There may be a perfectly good explanation. But it does mean you need to stop, ask questions, and involve Compliance before you go further.

[On screen: During the relationship]

Once a third party is on board, due diligence doesn't end. Every contract must include our anti-bribery clauses and the right to audit. Invoices should clearly describe the services provided. If an invoice just says "consulting services" and a large number, ask for details before it's approved.

And keep an eye on how the relationship feels. If a partner seems to get approvals remarkably quickly where others struggle, that's worth a question too.

[On screen: If you have concerns]

If something doesn't look right, don't investigate on your own, and don't confront the partner. Report it to Compliance, or use the Candor Line if you prefer to stay anonymous. You'll be protected for raising a concern in good faith.

[On screen: Summary]

So remember. Check before you engage. Watch for red flags. Keep contracts and invoices clear. And when something seems off, speak up early.

Next, you'll review a sample partner file and decide which red flags need follow-up.

Speak Up Line

Ethics, whistleblowing · Adult (25-40) · Neutral American · 60 seconds

[On screen: The Candor Line]

Sometimes you see something at work that doesn't feel right, and you're not sure who to tell. Maybe it involves your manager. Maybe you're worried about what people will think.

That's what the Candor Line is for.

[On screen: 1-800-555-0187]

It's open twenty-four hours a day, every day of the year. You can call 1-800-555-0187, or report online using the Candor Line link at the top of the intranet homepage.

The service is run by an independent company. You can give your name, or stay anonymous. Either way, you'll get a report number, so you can check for updates and answer follow-up questions without revealing who you are.

Every report is reviewed. And anyone who raises a concern in good faith is protected from retaliation.

You don't need to be certain. If something seems wrong, it's worth a call.

Lockout Before You Reach In

Workplace safety rules, lockout procedures · Adult (40-55) · Neutral American · 90 seconds

[On screen: Lockout procedure]

A jam in the conveyor. It happens every week. The fix takes thirty seconds. And it's exactly the kind of job where people get badly hurt, because someone reaches in while the machine can still start.

That's why we use lockout. Every time. No matter how quick the job.

[On screen: Six steps]

Step one. Tell the people affected that you're shutting the machine down.

Step two. Shut it down using the normal stop controls.

Step three. Isolate every energy source. That means electrical, and also air, hydraulic pressure, springs, and anything that could move.

Step four. Put your own lock and tag on each isolation point. Your lock, your key. Nobody else's.

Step five. Release any stored energy. Bleed the air lines, block anything that could fall.

Step six. Verify. Try to start the machine. If it doesn't move, you're ready to work.

[On screen: Your lock, your key, your life]

When the job's done, clear your tools, make sure everyone's clear, and only then remove your lock.

Never remove another person's lock. And never skip a step because you're in a hurry. The machine doesn't know you're only going to be a second.

PPE Is Not Optional

Workplace safety rules, protective equipment · Adult (25-40) · Australian · 60 seconds

[On screen: Personal protective equipment]

On this site, personal protective equipment isn't a suggestion. It's a condition of entry.

[On screen: Minimum PPE]

The minimum is steel-capped boots, a hard hat, high-vis, and safety glasses. You'll need hearing protection wherever you see the blue sign, and gloves for handling any materials with sharp edges.

[On screen: Check it]

Check your gear at the start of every shift. A cracked hard hat, scratched glasses, or boots with the caps showing won't protect you. Swap them out at the store room. It costs you nothing.

[On screen: Wear it properly]

Wear it properly, too. Hearing protection doesn't work around your neck, and safety glasses don't work on top of your head.

If a visitor or a new starter isn't wearing the right gear, speak up. You won't be having a go at them. You'll be looking after a mate.

Everyone goes home at the end of the day. That's the whole point.

Reporting a Near Miss

Workplace safety rules, incident reporting · Adult (30-45) · Neutral American · 60 seconds

Cast: TECH SUPERVISOR

On screen: Example conversation

TECH Hey, got a second? Probably nothing, but something happened on line three.

SUPERVISOR Sure. What's up?

TECH A pallet slipped off the forks when Danny was lifting it. Came down about two feet from where I was standing. Nobody got hurt.

SUPERVISOR Okay. I'm glad you're both fine. Did you see what caused it?

TECH I think the pallet was cracked underneath. You couldn't see it from the top.

SUPERVISOR Right. That's exactly the kind of thing I want to hear about. Can you log it as a near miss in the safety app before the end of your shift?

TECH Yeah, I can. I wasn't sure it counted, since nothing actually happened.

SUPERVISOR That's what makes it a near miss. Nothing happened this time. If we look into it now, maybe we find a batch of bad pallets before one lands on somebody.

TECH Makes sense. I'll put in a photo too.

SUPERVISOR Perfect. And thanks for telling me. Seriously.

On screen: A near miss is a warning you get for free. Report every one.

Accurate Books and Records

Ethics, financial integrity · Adult (40-55) · Neutral American · 90 seconds

[On screen: Accurate books and records]

When people hear the phrase "financial fraud," they often picture something dramatic. Hidden accounts, forged signatures, millions of dollars.

Most problems with company records start much smaller.

A sale booked on March thirty-first when the customer didn't sign until April second, to hit the quarterly target.

A client dinner recorded as a training expense because it's easier to get approved.

A timesheet rounded up by an hour, every week, because "everyone does it."

This matters. Each of these is a false record. Each one makes our financial reports less accurate. And accurate records are required by law, relied on by investors and auditors, and essential for making good business decisions.

[On screen: What we expect]

So we ask everyone to follow three simple rules.

Record transactions accurately, completely, and on time.

Never create or approve a record you know to be false or misleading, even if someone senior asks you to.

And never set up an account or fund that isn't recorded in the company's books.

If you're asked to do something that feels wrong, you can say no, and you can report it. You will be supported.

Inside Information

Ethics, confidential and inside information · Adult (30-45) · Neutral American · 90 seconds

[On screen: Inside information]

As part of your job, you may learn things about our company, or a company we work with, before the public does. An upcoming acquisition. A big contract win. Disappointing quarterly results.

That's called inside information. It's information that isn't public, and that a reasonable investor would likely consider important when deciding whether to buy or sell shares.

[On screen: The rules]

The rules are simple. If you have inside information, you must not buy or sell shares in the company it relates to. And you must not pass it on to anyone else, including friends and family, so that they can trade.

[On screen: Example]

Here's how it happens. You're at a barbecue, and your brother-in-law asks how work's going. You mention you've been working late on a "big deal with Corland Foods." The next morning, he buys shares in Corland.

You didn't trade. You didn't make any money. But you may still have broken the law, and so has he.

[On screen: If in doubt]

Insider trading can lead to serious fines and even prison.

So if you're ever unsure whether something counts, treat it as inside information and check with the Legal team before you do anything.

Annual Certification: Final Summary

Compliance, course summary · Adult (25-40) · Neutral American · 30 seconds

[On screen: Course complete]

You've reached the end of this year's compliance training. Thanks for your time and attention.

Before you go, remember the thread that runs through all of it. Protect the people and information we're trusted with. Act honestly. And when something doesn't seem right, speak up.

To finish, read the certification statement on the next screen and select I Agree. Your completion will be recorded automatically.

Travelling with Company Devices

Security awareness, business travel · Adult (30-45) · Australian · 90 seconds

[On screen: Travelling with company devices]

Laptops and phones get lost, stolen, and snooped on far more often when they're away from the office. Here's how to keep yours, and the information on it, safe on the road.

[On screen: Before you go]

Before you go, make sure your laptop is fully updated and your files are backed up. If you're travelling to a higher-risk country, check with the IT team. They may give you a loan device with only what you need.

[On screen: At the airport]

At the airport, keep your laptop with you, not in checked luggage. At security, watch it go through the scanner and pick it up straight away.

[On screen: Public wi-fi]

On public wi-fi, whether it's the hotel, the café, or the airport lounge, always turn on the company VPN before you do anything else. And be careful with charging stations. Use your own charger and a power point where you can.

[On screen: In public]

In public, watch what's on your screen. Trains and planes are full of people who can read over your shoulder. A privacy screen filter helps.

[On screen: If it's lost]

And if a device is lost or stolen, report it to the IT service desk as soon as possible, day or night. They can lock and wipe it remotely, but only if they know.

Competition Law at the Trade Show

Ethics, fair competition role-play · Adult (40-55) · Neutral American · 60 seconds

Cast: RAY JOANNA

On screen: Scenario - Evening reception at a trade show

RAY Joanna! Good to see you. How's life at Northfield?

JOANNA Busy, but good. How are things with you?

RAY Can't complain. Listen, while I've got you. Raw material costs are killing everyone this year, right?

JOANNA They've been tough, yes.

RAY So we're thinking of putting prices up about eight percent in January. Just between us, where are you landing? Because if we both go up, nobody loses customers.

JOANNA Ray, I'm going to stop you there. I can't talk about our pricing plans with you.

RAY Come on, it's just a chat. Nobody's writing anything down.

JOANNA I know, and I'm not trying to be awkward. But that's a conversation competitors can't have. Not at a bar, not anywhere.

RAY Fair enough. No harm meant.

JOANNA None taken. I'm going to grab some food. Enjoy the rest of the show.

On screen: What Joanna did next

JOANNA Hi, it's Joanna. I'm calling to report a conversation at the trade show tonight. A competitor raised future pricing. I stopped the conversation and left. I'd like to make sure it's on record.

On screen: Key points

On screen: Never discuss prices, costs, bids, customers, or territories with competitors.

On screen: If it comes up, stop it clearly, leave, and report it to Legal the same day.

On screen: Informal settings count. So do social events and industry associations.

The Consequences Slide

Compliance, accountability · Adult (40-55) · Neutral American · 30 seconds

[On screen: Why it matters]

Breaking the policies in this course can have serious consequences.

For the company, that can mean heavy fines, lost contracts, and damage to the trust our customers place in us. For individuals, it can mean disciplinary action, up to and including termination. Some violations can also lead to personal fines or criminal charges.

But the goal of this training isn't to scare you. It's to make sure you know the rules, and know you can always ask.

Your Rights Over Your Data

Data privacy, individual rights · Adult (25-40) · Neutral British · 2 minutes

[On screen: Individuals' rights]

People whose personal data we hold have rights over that data. Customers, employees, job applicants, even people who've simply emailed us.

Here are the ones you're most likely to come across.

[On screen: Access]

The right of access. Anyone can ask for a copy of the personal data we hold about them. This is often called a subject access request.

[On screen: Correction]

The right to have inaccurate data corrected. If a customer tells us their address is wrong, we fix it.

[On screen: Deletion]

The right to have data deleted, in certain circumstances. For example, when we no longer need it for the reason we collected it.

[On screen: Objection]

The right to object. Most commonly, someone asking us to stop sending them marketing emails. That request must always be honoured.

[On screen: How to spot a request]

Here's the tricky part. Requests rarely arrive with a helpful label. A customer might say, in the middle of a complaint, "and I want to see everything you've got on me." That's a subject access request. It doesn't need to use the official words, and it can arrive by phone, by email, through social media, or in person.

[On screen: What to do]

So if you think you've received one, don't try to handle it yourself. Log it straight away using the Privacy Request form on the intranet, and let the person know it's been passed to the right team.

Why the urgency? Because in most cases, we have one calendar month to respond. That clock starts on the day the request reaches anyone in the organisation, not the day it reaches the privacy team.

[On screen: Be polite, be quick]

Be polite, and never ask why they want the information. They don't have to tell us. Our job is simply to make sure their request reaches the people who can help.

Practice with these, record them, post them as demos or reels, use them in auditions. Please do not resell them as scripts. © VO Journey Academy · avosjourney.com