CYBEHAVE ACADEMY · SPECIALIST

Writing Policy People Follow

Course workbook

Plain language, defaults, and testing a policy before you publish it.

Build Behaviour. Build Culture. Build Resilience.

This workbook belongs to

Organisation and role

The policy I will work on through the course

cybehave.com/training · © 2026 CyBehave. All rights reserved. For use alongside the Writing Policy People Follow video course.

BEFORE YOU START

How to use this workbook

This is the specialist course for the people who turn standards into words that somebody will read on their first morning and act on in their third year. The workbook follows the eight videos in order, holds every template the videos refer to, and ends with the six quizzes and their answers. By the end you will have inventoried one page of a policy, brought it to a reading age a busy person can manage, audited it for clauses that should be system defaults, tested it on five readers, structured it in layers with a register, and attached a behaviour measure to every rule.

Five ways to get the most from it

1. **Bring one policy.** The one you own that matters most, or the one you are about to publish. Every section has a "Your policy" box.
2. **Inventory before you rewrite.** Module 1's test (can a reader act on this?) removes half the length before you touch a sentence.
3. **Use the numbers.** Reading age, sentence length, must count, day-one test result: a gate with numbers ends arguments about taste.
4. **Take the quizzes.** Scenarios, not definitions. Check the key and read the explanation for anything you missed.
5. **Do one thing per module.** Inventory a page. Run the tool. Audit for defaults. Book the test. Start the register. Attach a measure.

The course at a glance

Module	Title	Tools in this workbook
0	Welcome	The policy nobody reads; meet Daniel.
1	A Policy Is a Set of Behaviours	The three-readers sheet; the one-behaviour-per-clause inventory.
2	Plain Language That Can Be Done	The plain-language checklist; the before-and-after sheet; the publication gate.
3	Defaults, Not Instructions	The clause-to-default audit; the design-request form.
4	The Day-One Test	The test plan; the test log; the stop-line agreement; the policy-walk notes.
5	Structure, Versioning and Retirement	The layered template; the one-page role sheet; the register; the change-note template.
6	Measuring Compliance by Behaviour	The clause measure sheet; the three-fates sorter; the HEROES map.
7	Close	Six ideas; Monday list; glossary; further reading; quiz answers.

Three lines you will hear again

One behaviour per clause, with the reason beside it. · If it can be a default, it is not a policy. · Test it on five readers before you publish it to five thousand.

WORKED EXAMPLE

Meet Daniel

Daniel Okoro is information governance lead at Whitmore University: 4,800 staff, 22,000 students, nine faculties, 1,100 research staff with collaborators in forty countries. He arrived from a council where he took a policy estate of sixty documents to fourteen. At Whitmore he found sixty-one policies, an acceptable use policy of forty-seven pages with the word "must" two hundred and twelve times, 98% attestation, and analytics showing that 0.4% of readers scrolled past page two. The course follows his first year.

The five threads the course returns to
The forty-seven pages (modules 1, 2, 5): inventoried to 38 behaviours in one afternoon with a lecturer, a research administrator and a technician; rewritten from a reading age of 16 to 10; restructured as a one-page sheet per reader plus four pages of rules. "Must" from 212 to 38.
The password clause (module 3): fourteen characters, sixty days, no reuse of twenty-four, written in 2014 and signed every year since. Replaced by a default (single sign-on, a second factor, no forced expiry, a password manager) and three sentences. Helpdesk resets down 58%.
The day-one test (module 4): five new starters asked to find the rule for sharing with an external collaborator; one of five found it, in six minutes twenty. After the rewrite, five of five in forty seconds. Three rounds for the whole policy.
Attestation against behaviour (module 6): 98% attested; 31% of external sharing by the approved route. After the rewrite and the default: 79%. "I know what the rule is and why": 46% to 77%.
Retirement (module 5): sixty-one policies to eleven; fourteen clauses retired with reasons, nine converted to defaults; six one-page role sheets; a change note from the vice-chancellor with a 71% open rate against 9%.

Use Daniel as a mirror

Each time a Whitmore card appears, ask: what is my equivalent? How many pages, how many musts, what reading age, how many of five could find the rule, and what is the behaviour behind my attestation rate?

MODULE 1

A Policy Is a Set of Behaviours

Key ideas from the video

- A policy is for telling a person what to do, when, and why. The shield for the regulator and the artefact for the auditor are side effects of a policy that works, not the policy.
- Three readers: the person doing the job (ninety seconds, a task half done), the manager (ten minutes, once), the auditor and the lawyer (all day, a checklist). Write for the first; serve the others in layers.
- One behaviour per clause: a verb, a reader, a moment, and the reason beside it. If it needs two verbs, it is two clauses. The reason is what makes the rule survive the first time it is inconvenient.
- The test: can a reader act on this today without asking anyone? Yes: keep and rewrite. Yes but the system should do it: a default. No: a design request, or delete it. Most policies lose half their length here.
- Less is more: over two hundred experts gave 152 different pieces of advice; a shorter set is easier to follow. Ten behaviours a person can hold is a policy; two hundred and twelve "musts" is a hope.

Template: the three readers

Reader	What they need from this policy	How long they have	Where they will read it	Which layer serves them
The person doing the job				
The manager				
The auditor and the lawyer				

Template: the one-behaviour-per-clause inventory (one page of your policy)

Clause (as written)	The verb	The reader	The moment	The reason	Can they act on it? keep / default / request / delete

Clause (as written)	The verb	The reader	The moment	The reason	Can they act on it? keep / default / request / delete

Two hundred and twelve musts

One afternoon, one lecturer, one research administrator, one IT technician. Can act on it: 38. Should be a default: 9. Needs a tool nobody has: 6, sent to IT as design requests. Nobody could say what it meant: 159. The 38 grouped by reader: anyone 14, researchers 9, managers 6, IT 5, students 4.

The 159 went into an appendix titled "retired, with reasons", published alongside the new policy. Three people asked about three of them. Daniel to the committee: "We have not weakened the policy. We have found it."

Your policy

Inventory one page of your policy on the table above. How many clauses survive the test?

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Take one page of a policy you own. For each clause, write the behaviour it asks for as a verb, the reader it asks it of, and the reason. How many clauses survive?

2. Who was in the room when that policy was last revised: legal, audit, risk, a committee? Was anyone who has to follow it there?

3. Count the clauses on that page that a reader could act on today without asking anyone. What stops them acting on the rest?

4. Which clauses exist because of one incident years ago, and does anyone remember which?

5. If you could keep only ten behaviours from the whole policy, which ten, and what would you do with the other two hundred?

Module 1 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. According to the course, what is a policy for?

A Providing legal protection for the organisation

B Satisfying the auditor's checklist

C Recording every incident that has ever happened

D Telling a person what to do, when, and why; the shield for the regulator and the artefact for the auditor are side effects of a policy that works

2. Who are the three readers of a policy, and which one should it be written for?

A Staff, students and contractors; write for staff

B IT, HR and legal; write for legal

C The person doing the job, the manager, and the auditor or lawyer; write for the first and serve the other two in layers

D The author, the committee and the regulator; write for the regulator

3. The clause reads: "Users must ensure that all information assets are handled in accordance with their classification at all times." What is wrong with it, in the course's terms?

A Nothing; it is a standard clause

B It asks for three or four behaviours at once, of everyone, always, for reasons the reader has to go and find; nobody can act on it

C It is too short

D It uses the word "must"

4. What is the "can a reader act on this?" test, and what are the three fates?

A Ask whether a reader could act on the clause today without asking anyone: yes (keep, rewrite in the pattern), yes but the system should do it (a default), or no (a design request, or delete it)

B Ask legal whether the clause is enforceable: keep, amend or escalate

C Ask the committee whether they are comfortable: approve, defer or reject

D Ask the author whether it is complete: publish, revise or archive

5. Reeder, Ion and Consolvo asked over two hundred security experts for their top three pieces of advice. What did they find, and why does the course cite it?

A All experts agreed on the same three; policies should copy them

B Experts recommended longer policies

C Experts could not name any advice

D 837 answers and 152 different pieces of advice with no consensus; a shorter set is easier to follow, so a policy with 212 "musts" is a hope, not a policy

6. Daniel's inventory of the acceptable use policy reduced 212 "musts" to 38 behaviours. What did he do with the 159 clauses that nobody could act on?

A Moved them to a separate mandatory policy

B Converted them all into training modules

C Published them in an appendix titled "retired, with reasons" alongside the new policy, so nobody could say the rules had been lost

D Deleted them silently

MODULE 2

Plain Language That Can Be Done

Key ideas from the video

- The GOV.UK standard: plain English is mandatory; aim for a reading age of nine; keep sentences under about twenty-five words. The reason is speed, not ability: even expert readers prefer plain text they can scan.
- Verbs over nouns: "ensure", "appropriate", "in accordance with", abstract nouns and the passive voice all hide the behaviour. Delete them and the verb appears, with the person and the moment.
- Must, should and may used honestly. A must has a consequence you will apply; most policies have about ten. Two hundred and twelve musts means none of them is one.
- Every must has its reason in the same sentence or the next. A rule with its reason is followed when nobody is watching.
- The gate: the ten-second test, the readability tool (reading age twelve or under, no sentence over thirty words), defined terms a new starter knows, a must count, a reason check. Numbers, not taste.

Template: the plain-language checklist (one clause)

Check	Yes / no	Fix
One verb, one reader, one moment		
Under twenty-five words		
No "ensure", "appropriate", "in accordance with", no passive		
Words the reader would use in the kitchen		
Must / should / may used honestly		
The reason, in this sentence or the next		
Passes the ten-second test with somebody in the role		

Template: before and after

Before (as written, word count)	After (verb, reader, moment, reason, word count)

Before (as written, word count)	After (verb, reader, moment, reason, word count)

The publication gate

Measure	Limit	This policy
Reading age (readability tool)	12 or under	
Longest sentence	30 words	
Must count	Under 40 (aim for 10 to 20)	
Defined terms a new starter would not know	0	
Musts without a reason	0	

Sixteen to ten

Baseline: reading age 16; longest sentence 61 words; 212 musts; 44 defined terms, 31 unknown to a new starter. After the rewrite, with two readers reading every clause aloud: reading age 10; longest sentence 24; 38 musts, each with its reason; 6 defined terms, all defined where they appear. Legal's concern ("it no longer sounds like a policy") answered by the detail layer, one click behind every rule.

Reporting went from thirty-six words and a cross-reference to "press Report or ring 4444; do it straight away." Reports rose by a third the following quarter, before any campaign. "Nobody had been refusing to report. They had been unable to find out how."

Your policy

Paste your policy into a readability tool. Write the reading age and the longest sentence here, then rewrite three clauses on the before-and-after sheet.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Run your policy through a readability tool. What reading age does it report, and what is its longest sentence?

2. Find three clauses that use "ensure", "appropriate" or "in accordance with". Rewrite each as a verb a reader can do.

3. Count the "musts", "shoulds" and "mays" in one section. Is each one honest about whether the rule is a rule?

4. Which defined terms in your policy would a new starter not know? What would you call them in conversation?

5. Read one clause aloud to somebody who has the role and give them ten seconds. Can they tell you what to do?

Module 2 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. What does the GOV.UK standard quoted in the module say about reading age and sentence length?

A Sentences should be as long as needed for legal precision

B Reading age does not matter for policy documents

C Plain English is mandatory; aim for a reading age of nine; keep sentences under about twenty-five words

D Aim for a reading age of sixteen to maintain authority

2. Why does the course say plain language is "not dumbing down"?

A Because readability tools are unreliable

B Because it is writing so that an intelligent person with ninety seconds and a job to do can find the rule, understand it and act, first time

C Because it is only for junior staff

D Because it removes all the rules

3. Which word hides the behaviour in "Users must ensure that devices are locked"?

A "Ensure", which asks nobody to do anything; "Lock your screen when you leave your desk" does

B "Users"

C "Devices"

D "Locked"

4. What does the course say about a policy with two hundred and twelve "musts"?

A It is admirably thorough

B Each must should be converted to "shall"

C The number is irrelevant as long as each is justified

D None of them is a must; a "must" nobody enforces teaches that none of them count, and if there are more than twenty, some are shoulds, some are defaults and most are guidance

5. What is the ten-second test?

A Readers must sign within ten seconds

B Each clause must be under ten words

C Read one clause aloud to somebody with the role; ten seconds later ask what they would do; if they cannot say, rewrite

D A policy must load in under ten seconds

6. When Daniel rewrote the reporting clause from thirty-six words and a cross-reference to "press Report or ring 4444; do it straight away", what happened to reports the following quarter?

A They rose only after a poster campaign

B They rose by a third before any campaign; nobody had been refusing to report, they had been unable to find out how

C They fell because the clause was less formal

D Nothing changed

MODULE 3

Defaults, Not Instructions

Key ideas from the video

- If it can be a default, it is not a policy. Passwords, screen lock, encryption, updates, forwarding, expiring links, a second factor: a person should not be asked to remember what a system could enforce once, for everyone.
- The password clause from 2014 (fourteen characters, sixty days, no reuse of twenty-four) asked for the impossible and everyone attested to it. National guidance now: do not force regular expiry; change on a trigger; use a second factor. It became a default plus three sentences.
- The clause-to-default audit has three columns: already enforced (delete the clause), could be enforced (a design request, not a rule), needs a person (the policy).
- What remains is the judgement calls: sharing, requests to break a rule, reporting and what happens to you, visitors and contractors, exceptions, and the reasons. Shorter, and every sentence about a decision.
- Run the audit with the architects in the room. Each learns what the other has been assuming.

Template: the clause-to-default audit

Clause	Already enforced (delete)	Could be enforced (design request to whom)	Needs a person (keep, rewrite)	Action and date

Template: the design request

Line	Entry
The clause as written, and the behaviour it asks for	

Line	Entry
The system that could enforce it	
The policy's reason, attached	
Owner of the system; date sent	
Until built, the clause is: withdrawn / marked "guidance" / kept with a note	

Nine defaults and six requests

Already enforced, deleted: 4 (screen lock, laptop encryption, update deadlines, forwarding to personal accounts). Could be enforced, sent as design requests: 6, including expiring sharing links, a second factor on two legacy systems, and the password clause. Needs a person: 23, now the whole of the rules layer.

The password default shipped in month four; the policy kept three sentences; helpdesk resets fell 58%. The head of IT: "I have been enforcing four of these for three years and the policy was still telling people to do them by hand." Every new clause is now tagged default, request or person before it is drafted.

Your policy

Run the audit on your policy. How many clauses are already enforced, and who gets the design requests?

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Go through one policy and mark every clause a system could enforce instead of a person remembering. How many are there?

2. Which of those clauses is the system already enforcing, so the clause is dead weight, and which is it not, so the clause is a design request?

3. Take your password clause. What does the national guidance now say, what does your system do, and what does your policy still ask a person to remember?

4. Who owns the systems your defaults would live in, and have they ever seen the policy that assumes them?

5. What is left for the policy to say once the defaults are out: which judgement calls, which exceptions, which reasons?

Module 3 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. What is the rule at the heart of module 3?

A Defaults are the IT department's problem and have nothing to do with policy

B If it can be a default, it is not a policy clause: a person should not be asked to remember what a system could enforce once, for everyone

C Every default should also be a policy clause for completeness

D Policies should describe every system setting

2. What does the national guidance quoted in the module say about forced regular password expiry?

A Do not force it: it pushes people to weaker, predictable passwords and buys little; change on a trigger such as suspected compromise, and use a second factor

B Change passwords every thirty days

C Change passwords every sixty days with no reuse of the last twenty-four

D Passwords should never be changed

3. In the clause-to-default audit, what happens to a clause the system already enforces?

A Keep it so the policy is complete

B Move it to a stricter policy

C Add a penalty for non-compliance

D Delete it from the policy, keeping at most one sentence of explanation; it is dead weight

4. What remains for the policy once the defaults are out?

A Only the legal disclaimers

B A list of system settings

C The judgement calls: who you may share what with, what to do when somebody asks you to break a rule, when and how to report, exceptions, and the reasons

D Nothing; the policy can be retired

5. Why does the course recommend running the audit with the architects in the room?

A Because it is a regulatory requirement

B Because each learns what the other has been assuming: IT had been enforcing four clauses the policy still asked people to do by hand, and two the policy asked for had never been requested

C Because architects must approve all policy changes

D Because the policy owner cannot read system configurations

6. What happened to helpdesk password resets after the password default shipped?

- **A** They fell by 58%
- **B** They rose, because people forgot their new passwords
- **C** They were unchanged
- **D** The helpdesk stopped counting them

MODULE 4

The Day-One Test

Key ideas from the video

- The question is not "is it correct" but "can a new starter find the rule and act on it, on day one, with a task and a minute". Policies are reviewed by everyone except that reader.
- Five readers with the role (at least two in their first three months), three tasks written as situations, one at a time, thinking aloud, on their own device, no help until two minutes stuck. Ninety minutes.
- Write down six things: found the rule or not; time to find; what they said they would do; whether it matched; where they looked first; the words they used.
- The stop line (for example four of five find each rule in under sixty seconds and would do what it says) is agreed before the test with whoever can delay publication. Fix the top three problems, retest with five new readers, publish with the result in the change note.
- The policy walk: once a quarter, an hour with a real new starter in their first week, ideally by a Champion. It finds the rules nobody looks up and the induction slide that contradicts the policy.

Template: the day-one test plan

Line	Entry
The policy and version under test	
Task 1 (as a situation)	
Task 2	
Task 3	
The five readers (role, tenure), none involved in writing it	
The stop line, and who agreed it	
Date, facilitator, note-taker	

Template: the day-one test log (one task)

Reader	Found it? (Y/N)	Time to find	What they said they would do	Matched the rule? (Y/N)	Where they looked first	Words they used
1						
2						
3						
4						
5						

Template: the policy walk

Moment in the first week where the policy applied	What they did	What they looked at	Finding: clause to rewrite / default to request / slide to fix

One of five, then five of five

Task one, the old policy: "a collaborator in Lisbon needs this spreadsheet." One of five found the rule; median six minutes twenty for the one who did; four would have emailed it. Three searched for "email", one for "share", one gave up. The rule was under "Information Handling: External Transfers" and used neither word. Stop line, agreed with the committee chair: four of five in under sixty seconds. The policy went back with the readers' sentences on page one of the paper.

After the rewrite ("Sharing files with people outside the university: use the sharing tool, not email"): five of five, median forty seconds. Three rounds for the whole policy. The committee chair: "We have approved this policy four times. This is the first time anyone has shown me a person using it."

Your policy

Write your three tasks and your stop line, and name the five readers.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. Write three tasks a new starter will face in their first month that your policy is supposed to answer. Could you find the answer in under a minute yourself?

2. Who are the five readers you will test with, and which of them has been in the organisation less than three months?

3. What is your stop line: how many of five must find the rule, in what time, before you publish?

4. When did a policy in your organisation last go back for a rewrite because of something a reader did, rather than something a reviewer said?

5. Who could run the day-one test routinely: Champions, the induction team, the policy owner? What would it take to make it a step in publication?

Module 4 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. What is the question the day-one test answers?

A Can a new starter find the rule and act on it, on day one, with a task and a minute; not "is it correct"

B Is the policy legally defensible?

C Does the policy map to the standard?

D Is the committee comfortable approving it?

2. How are the test tasks written?

A As clause numbers to locate

B As multiple-choice comprehension questions

C As a reading-speed exercise

D As situations a new starter will actually face ("a collaborator in Lisbon needs this spreadsheet"), not as clause numbers

3. What is the stop line, and when must it be agreed?

A The policy's publication deadline

B The point at which the facilitator may help

C A pass threshold such as "four of five find each rule in under sixty seconds and would do what it says", agreed with whoever can delay publication, before the test

D The end of the ninety-minute session

4. Why five readers?

A Because more would take too long

B The same usability finding that applies to controls and web forms: five find most of the serious problems and the sixth mostly repeats them; fix, then test five more

C Because five is the statistical minimum for significance

D Because five is the committee size

5. In Daniel's first day-one test, four of five readers said they would email the spreadsheet. Where had they looked for the rule?

A Three searched for "email", one for "share", one gave up; the rule was under "Information Handling: External Transfers" and used neither word

B They did not look at all

C They found the rule but disagreed with it

D They looked in the HR handbook

6. What is the policy walk?

A A guided tour of the policy document for new starters

B An annual audit of the policy by legal

C A walkthrough of the policy by its author to the committee

D Once a quarter, sitting with a real new starter for an hour in their first week and watching what they do and look at whenever the policy applies; ideally run by Champions

MODULE 5

Structure, Versioning and Retirement

Key ideas from the video

- Three layers, one per reader: the one-page role sheet (ten or so behaviours, each a verb with its reason, and the reporting route); the rules (four to six pages, grouped by situation); the detail (the mapping, definitions, exceptions, procedures). Every line links down.
- Fewer policies: sixty-one is a place rules go to hide. Group by what the reader is doing, merge the overlaps, demote procedures and standards to layer three, retire what a system enforces or nobody follows.
- The register: owner by name, readers served, last and next review with the day-one test result, the behaviour measure, clauses retired or converted in the last year, and a sunset date for anything written after a single incident.
- Retirement is harder than addition because nobody is blamed for a clause that stayed. Make it a normal, logged, reasoned event with a published "retired, with reasons" appendix.
- Two change notes every time: the reader's first ("three things changed for you", four sentences, from the most senior voice), then the auditor's (version table, mapping, approvals) in layer three.

Template: the one-page role sheet

Role: _____	
1 (verb, moment) because (reason)	links to rule
2	
3	
4	
5	
6	
7	
8	
9	
10	
If something goes wrong: press Report / ring ____. Do it straight away.	

Template: the register

Policy	Owner	Readers / role sheets	Last review (day-one result)	Next review	Behaviour measure (latest)	Retired / converted this year	Sunset date

Template: the change note for readers

Sentence	Yours
1 What changed for you (the one or two things that matter most)	
2 What you no longer have to do	
3 Where to find the rest (the role sheet, the rules, one link)	
4 How to report, and what happens to you when you do	
Signed by (the most senior voice who will say it out loud)	

Sixty-one to eleven

Nineteen merged, twenty-two demoted to layer three, nine retired outright. Six one-page role sheets: staff, researcher, student, manager, IT, contractor; the researcher sheet translated into the three languages of the largest collaborations. A register of eleven rows with an owner, a review date, a measure, and a sunset date on the four written after single incidents. Fourteen clauses retired with reasons; three queries, all answered by the appendix line.

The change note from the vice-chancellor, four sentences with the researcher sheet attached: 71% open rate against 9% for the previous version notice. "A policy nobody can find is not a control. It is a document."

Your policy

Draft the role sheet for the role that matters most, and start the register with your policy as row one.

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. How many security-related policies does your organisation have, and could you name them all? How many could a new starter name?

2. Sketch the layered version of your main policy: what goes on the one-page role sheet, what in the rules, what in the detail. What is left over?

3. Open your policy register, or start one. For each policy: owner, last review, next review, and the last time anyone retired a clause.

4. Take your last change note. Was it written for the auditor ("v3.2, section 4 amended") or for the reader ("you can now share drafts with collaborators using the tool")?

5. Which clause would you retire first, and what would the change note say?

Module 5 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. What are the three layers of a layered policy, and who is each for?

A Draft, approved and archived versions

B Policy, standard and procedure, all for everyone

C Summary, body and appendix, all for the committee

D A one-page role sheet for the person doing the job; the rules (four to six pages) for the manager and the curious; the detail (as long as it needs to be) for the auditor and the lawyer

2. Why does the course say sixty-one policies is "a place rules go to hide"?

A Because policies should be numbered differently

B Because the regulator prefers fewer documents

C A reader cannot know which applies, overlapping policies contradict each other, sixty-one do not get owners and reviews, and the compliance budget is spent finding the rule rather than following it

D Because sixty-one is an odd number

3. Which is a column in the register the course describes?

A The committee that first approved it in 2009

B A sunset date for anything written in response to a single incident: review in a year, retire unless the reason still stands

C The number of pages

D The font used

4. What is the "retired, with reasons" appendix for?

A Every clause removed is listed with one line on why, published alongside the policy, so that retirement is a normal, logged event and nobody can say the rules were lost

B A confidential record for legal

C A list of staff who failed to follow the old clauses

D A draft of next year's policy

5. How does the course say a change note should be written?

A As "v3.2: sections 4.1 to 4.9 amended"

B Only for the auditor; readers do not need one

C As a full reprint of the policy

D For readers first: "three things changed for you", in plain sentences, before the version table and mapping for auditors in layer three

6. How did Daniel get from sixty-one policies to eleven?

A He combined them all into one document

B He outsourced them to a consultancy

C Nineteen merged, twenty-two demoted to layer three as procedures and standards, nine retired outright, and the rest grouped by what the reader is doing

D He deleted fifty at random

MODULE 6

Measuring Compliance by Behaviour

Key ideas from the video

- Attestation measures the process: a document sent, a click recorded, an auditor satisfied. Behaviour measures the policy. Keep the first if the auditor needs it; report the second.
- One measure per clause, from four sources: a system count (shares by tool against attachments; reports and latency), a Team Pulse item ("I know what the rule is and why"; observed behaviour), an audit sample (ten desks, ten leavers), the day-one test.
- A rule with no measure is one you cannot defend, improve or retire. If no measure exists, ask whether the rule does.
- The clause nobody follows has three fates: fix it (not found or understood), make it a default (understood but too costly), remove it (understood, possible, not done, no harm). Never "more training" first.
- In HEROES: each role-sheet rule as a behaviour with its measure; the Team Pulse items; the rewrite as an intervention; the change note as a campaign; Champions' tests as tasks; behaviour on the board pack. The documents stay with the owner.

Template: the clause measure sheet (one role sheet)

Rule (from the role sheet)	Measure	Source: system / Team Pulse / audit sample / day-one test	Baseline	Latest	Fate if low: fix / default / remove

Template: the three-fates sorter

Clause with low behaviour	Found? Understood? Possible? Harm if not done?	Fate	Action, owner, date

Template: the HEROES map

This course	In HEROES	Ours
Each rule on a role sheet	Behaviour in the catalogue, with its measure as a direct measure	
"I know what the rule is and why"; observed behaviour	Team Pulse items, quarterly, by team	
The rewrite	Intervention record, with COM-B driver and APEASE pass	
The change note and the role sheet	Campaign	
Day-one tests and policy walks	Champion tasks	
The policy documents, the register, attestation records	Not in HEROES: kept by the policy owner	

Thirty-one to seventy-nine

Baseline: attestation 98%; external sharing by the approved route 31% (tool shares against external attachments, from the logs); day-one test one of five. After the rewrite and the tests: 52%. After expiring links as a default and the sharing button in the mail client: 79%. No campaign beyond the change note. Eleven policies, each main rule with a measure: nine system counts, six Team Pulse items, four audit samples. "I know what the rule is and why": 46% to 77%.

Three low rules at year end: one fixed (a heading), one made a default (encryption on a legacy fleet), one removed (a visitor-log clause nobody had followed since the badge system). The slide that replaced the attestation report: eleven policies, a number beside each main rule, moving quarter on quarter; attestation in a footnote.

Your policy

Attach a measure to each rule on your role sheet. Which rules have none, and are they really rules?

Reflect & apply

Pause the video and take ten minutes with these. Write, do not just think.

1. What is your attestation rate, and what is the behaviour rate for your three most important clauses? If you only know the first, what would it take to know the second?

2. For each clause on one role sheet, name a measure: a count from a system, a Team Pulse item, an audit sample. Which clauses have none, and are they really rules?

3. Which clause in your estate has the lowest behaviour rate? Is the fix the clause, a default, or removal?

4. Which of your clause measures could appear in HEROES beside the programme's behaviours, and who would read them?

5. What would your annual policy review look like if it started from the behaviour measures rather than from the document?

Module 6 quiz

Six questions, one answer each. Four of six is a pass. The same quiz is on the training page under the video; the answers and explanations are at the back of this workbook.

1. What does a 98% attestation rate tell you, according to the course?

A That the policy is well written

B That training has been effective

C That the system sent a document and recorded a click, that people know the click keeps their access, and that the auditor will be satisfied; nothing about what anyone does on a Tuesday

D That 98% of staff follow the policy

2. Which of these is one of the four sources of a per-clause measure described in the module?

A The length of the policy

B A Team Pulse item such as "I know what the rule is and why", or colleagues rating observed behaviour

C The number of times the policy was downloaded

D The attestation rate

3. A clause is understood and possible, yet still not followed, and no harm results. What fate does the course give it?

A Remove it: it was never worth its budget; retire it with the reason and spend the budget on a rule that is

B More training

C A disciplinary process for non-compliance

D Move it to a stricter policy

4. Why does the course say "more training" is almost never the answer to a clause nobody follows?

A Because training is too expensive

B Because staff refuse to attend

C Because training is HR's responsibility

D Training a rule that cannot be found, done or justified teaches people that the policy is noise; it is the last lever, not the first

5. Which of these lives in HEROES, per the platform mapping?

A The attestation records

B The committee minutes

C Each role-sheet rule as a behaviour with its measure, the Team Pulse items, the rewrite as an intervention, the change note as a campaign, and Champions' day-one tests as tasks

D The policy documents and the register

6. External sharing by the approved route went from 31% to 79% at Whitmore. What produced the second half of the rise?

A A longer policy with more detail

B Expiring links shipped as a default and the sharing button appearing in the mail client, in month six, with no campaign beyond the change note

C A poster campaign

D Disciplinary action against people who emailed attachments

CLOSE

Close: What to Do on Monday

The course in six lines

1. **A policy is a set of behaviours.** Three readers; one behaviour per clause, with the reason; the "can a reader act on this" test; less is more.
2. **Plain language that can be done.** Reading age ten, short sentences, verbs not nouns, must and should used honestly, a gate with numbers.
3. **Defaults, not instructions.** If it can be a default, it is not a policy. Audit every clause: enforced, could be, needs a person.
4. **The day-one test.** Five readers, three tasks, a stopwatch, a stop line agreed before. Fix, retest, publish with the result.
5. **Structure, versioning and retirement.** Three layers; fewer policies; a register; retire with reasons; change notes for readers.
6. **Measuring compliance by behaviour.** One measure per clause; three fates for a low one; the behaviours in HEROES.

Monday

Done	This week
☐	Inventory one page of one policy: verb, reader, reason, and the "can they act on it" test
☐	Paste the whole policy into a readability tool and write down the reading age and the longest sentence
☐	Mark every clause a system could enforce, and take the list to whoever owns the system
☐	Book a day-one test with five readers for the next policy you publish, and agree the stop line
☐	Start the register
☐	Write the next change note for the reader first, in four sentences, before the one for the auditor

Glossary

Term	Meaning in this course
The three readers	The person doing the job, the manager, the auditor and lawyer. Write for the first; serve the rest in layers.
One behaviour per clause	A verb, a reader, a moment, and the reason beside it.
The act-on-it test	Can a reader act on this today without asking anyone? Keep, default, request or delete.
Reading age	The readability tool's estimate of the schooling needed to read the text easily. Aim for nine to ten.
Must / should / may	A rule with a consequence; the expected default with room for judgement; a permission.

Term	Meaning in this course
The gate	Numbers a policy must pass before publication: reading age, sentence length, must count, defined terms, reasons.
Default	A behaviour the system enforces so the person does not have to remember it.
Design request	A clause the system could enforce but does not yet; sent to the system owner, not published as a rule.
Day-one test	Five readers, three tasks as situations, a stopwatch, a stop line agreed before.
Policy walk	An hour with a real new starter in their first week, watching where the policy applies.
Layered policy	Role sheet, rules, detail: one layer per reader, each linking down.
Register	One row per policy: owner, readers, reviews, measure, retirements, sunset date.
Retired, with reasons	The published appendix of removed clauses and why.
Behaviour measure	A per-clause number from a system count, a Team Pulse item, an audit sample or the day-one test.
The three fates	Fix the clause, make it a default, remove it. Never "more training" first.

Further reading

- GOV.UK. Writing for GOV.UK: clear language and plain English; Inside GOV.UK (2014), Sentence length: why 25 words is our limit.
- Plain English Campaign. plainenglish.co.uk.
- Reeder, R. W., Ion, I. and Consolvo, S. (2017). 152 simple steps to stay safe online: security advice for non-tech-savvy users. IEEE Security and Privacy, 15(5).
- Bada, M., Sasse, M. A. and Nurse, J. R. C. (2015). Cyber security awareness campaigns: why do they fail to change behaviour?
- Beautement, A., Sasse, M. A. and Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. NSPW 2008.
- Kirlappos, I., Parkin, S. and Sasse, M. A. (2014). Learning from "Shadow Security". USEC 2014.
- Nielsen, J. (2000). Why you only need to test with 5 users. Nielsen Norman Group.
- National Cyber Security Centre. Password guidance: simplifying your approach; The problems with forcing regular password expiry. ncsc.gov.uk.
- Michie, S., van Stralen, M. M. and West, R. (2011). The behaviour change wheel. Implementation Science, 6(42).
- CyBehave Academy: Behavioural Science for Security Architects; Psychological Safety and Reporting Culture; Running Behavioural Experiments; Security Communications That Change Behaviour.

Notes

ANSWER KEY

Quiz answers

Four of six is a pass. Read the explanation for every question you missed, then go back to the template it points at.

Module 1: A Policy Is a Set of Behaviours

#	Answer	Why
1	D Telling a person what to do, when, and why; the shield for the regulator and the artefact for the auditor are side effects of a policy that works	A document written for the shield and the artefact alone changes nobody's Tuesday.
2	C The person doing the job, the manager, and the auditor or lawyer; write for the first and serve the other two in layers	The person doing the job is the only reader whose behaviour the policy exists to change, and they have ninety seconds.
3	B It asks for three or four behaviours at once, of everyone, always, for reasons the reader has to go and find; nobody can act on it	One verb, one reader, one moment, one reason. If it needs two verbs, it is two clauses.
4	A Ask whether a reader could act on the clause today without asking anyone: yes (keep, rewrite in the pattern), yes but the system should do it (a default), or no (a design request, or delete it)	Run it with one person who has the role in one sitting. Most policies lose half their length here.
5	D 837 answers and 152 different pieces of advice with no consensus; a shorter set is easier to follow, so a policy with 212 "musts" is a hope, not a policy	Choose ten behaviours by consequence and frequency. Everything else is guidance, linked, for the reader who wants it.
6	C Published them in an appendix titled "retired, with reasons" alongside the new policy, so nobody could say the rules had been lost	Three people asked about three of them. His line to the committee: "We have not weakened the policy. We have found it."

Module 2: Plain Language That Can Be Done

#	Answer	Why
1	C Plain English is mandatory; aim for a reading age of nine; keep sentences under about twenty-five words	The reason is speed, not ability: research shows even expert readers prefer plain language they can scan.
2	B Because it is writing so that an intelligent person with ninety seconds and a job to do can find the rule, understand it and act, first time	A reader who has to read a clause twice does not read the next one.
3	A "Ensure", which asks nobody to do anything; "Lock your screen when you leave your desk" does	Ensure, appropriate, in accordance with, and the passive voice all hide the verb. Delete them and the verb appears.
4	D None of them is a must; a "must" nobody enforces teaches that none of them count, and if there are more than twenty, some are shoulds, some are defaults and most are guidance	A must is a rule with a consequence you will apply. Most policies have about ten.
5	C Read one clause aloud to somebody with the role; ten seconds later ask what they would do; if they cannot say, rewrite	Together with the readability tool, the must count and the reason check, it makes a publication gate with numbers, so nobody has to argue taste.

#	Answer	Why
6	B They rose by a third before any campaign; nobody had been refusing to report, they had been unable to find out how	The rewrite took the policy from a reading age of sixteen to ten, and the gate became four numbers in the publication process.

Module 3: Defaults, Not Instructions

#	Answer	Why
1	B If it can be a default, it is not a policy clause: a person should not be asked to remember what a system could enforce once, for everyone	Each such clause spends from the same compliance budget as the rules that genuinely need a person.
2	A Do not force it: it pushes people to weaker, predictable passwords and buys little; change on a trigger such as suspected compromise, and use a second factor	The 2014 clause asked for the impossible and everyone attested to it. It became a default plus three sentences.
3	D Delete it from the policy, keeping at most one sentence of explanation; it is dead weight	A clause the system could enforce but does not is a design request, not a rule, and should not be published as one until the system can.
4	C The judgement calls: who you may share what with, what to do when somebody asks you to break a rule, when and how to report, exceptions, and the reasons	A policy stripped of its defaults is shorter, and every sentence is about a decision a person has to make. That is a document people read.
5	B Because each learns what the other has been assuming: IT had been enforcing four clauses the policy still asked people to do by hand, and two the policy asked for had never been requested	At Whitmore the audit became a standing item: every new clause is tagged default, request or person before it is drafted.
6	A They fell by 58%	Single sign-on, a second factor everywhere, no forced expiry, a password manager offered; the policy kept three sentences.

Module 4: The Day-One Test

#	Answer	Why
1	A Can a new starter find the rule and act on it, on day one, with a task and a minute; not "is it correct"	Policies are reviewed by legal, risk, the committee and the author, and almost never by a reader with a task.
2	D As situations a new starter will actually face ("a collaborator in Lisbon needs this spreadsheet"), not as clause numbers	Three tasks, five readers with the role (at least two in their first three months), one at a time, thinking aloud, with the facilitator saying almost nothing.
3	C A pass threshold such as "four of five find each rule in under sixty seconds and would do what it says", agreed with whoever can delay publication, before the test	Agree it afterwards and it will be negotiated away. Below the line, the policy goes back with the readers' words.
4	B The same usability finding that applies to controls and web forms: five find most of the serious problems and the sixth mostly repeats them; fix, then test five more	Two rounds is normal; a third suggests the structure is wrong, which module 5 addresses.

#	Answer	Why
5	A Three searched for "email", one for "share", one gave up; the rule was under "Information Handling: External Transfers" and used neither word	After the rewrite, under the heading "Sharing files with people outside the university", five of five found it in a median of forty seconds.
6	D Once a quarter, sitting with a real new starter for an hour in their first week and watching what they do and look at whenever the policy applies; ideally run by Champions	It finds the rules nobody looks up, the induction slide that contradicts the policy, and the manager who says "ignore that bit".

Module 5: Structure, Versioning and Retirement

#	Answer	Why
1	D A one-page role sheet for the person doing the job; the rules (four to six pages) for the manager and the curious; the detail (as long as it needs to be) for the auditor and the lawyer	Every line on the sheet links to its rule; every rule links to its detail. The reader goes as deep as they need and no deeper.
2	C A reader cannot know which applies, overlapping policies contradict each other, sixty-one do not get owners and reviews, and the compliance budget is spent finding the rule rather than following it	Group by what the reader is doing, merge the overlaps, demote procedures to layer three, retire what a system enforces or nobody follows.
3	B A sunset date for anything written in response to a single incident: review in a year, retire unless the reason still stands	Also: owner by name, readers served, last and next review with the day-one test result, the behaviour measure, and clauses retired or converted in the last year.
4	A Every clause removed is listed with one line on why, published alongside the policy, so that retirement is a normal, logged event and nobody can say the rules were lost	Nobody is ever blamed for a clause that stayed, which is why taking one out is harder than putting one in.
5	D For readers first: "three things changed for you", in plain sentences, before the version table and mapping for auditors in layer three	At Whitmore the reader's note from the vice-chancellor, with the role sheet attached, had a 71% open rate against 9% for the previous version notice.
6	C Nineteen merged, twenty-two demoted to layer three as procedures and standards, nine retired outright, and the rest grouped by what the reader is doing	Plus six one-page role sheets and a register with an owner, a review date, a measure and, where relevant, a sunset date for each.

Module 6: Measuring Compliance by Behaviour

#	Answer	Why
1	C That the system sent a document and recorded a click, that people know the click keeps their access, and that the auditor will be satisfied; nothing about what anyone does on a Tuesday	Attestation measures the process; behaviour measures the policy. Keep the first if the auditor needs it, report the second.
2	B A Team Pulse item such as "I know what the rule is and why", or colleagues rating observed behaviour	The four: a system count, a Team Pulse item, an audit sample, and the day-one test result.
3	A Remove it: it was never worth its budget; retire it with the reason and spend the budget on a rule that is	The three fates: fix the clause (not found or understood), make it a default (understood but too costly), remove it. Never "more training" first.

#	Answer	Why
4	D Training a rule that cannot be found, done or justified teaches people that the policy is noise; it is the last lever, not the first	Low behaviour is information about the clause, not the person.
5	C Each role-sheet rule as a behaviour with its measure, the Team Pulse items, the rewrite as an intervention, the change note as a campaign, and Champions' day-one tests as tasks	The documents stay with the policy owner; the behaviour travels. The annual review starts from the measures, not the document.
6	B Expiring links shipped as a default and the sharing button appearing in the mail client, in month six, with no campaign beyond the change note	The rewrite and the day-one tests took it to 52%; the default took it to 79%. "I know what the rule is and why" rose from 46% to 77%.