New Dynamics

Policies and practice

Employee data protection: a policy planning guide

Map worker information, set access and retention responsibilities and draft a practical handling framework.

Practical guidance · Worked examples · Printable worksheet

New Dynamics Editorial Team
Published 15 September 2026

www.new-dynamics.com
contact@new-dynamics.com

Inside this guide

Read in order for the full approach, or use the linked contents to find a section. The final worksheet gives you space to record decisions and next steps.

Map worker information, set access and retention responsibilities and draft a practical handling framework. This practical guide to employee data protection brings together a step-by-step approach, illustrative examples, a reusable worksheet and answers to common questions. Start with the section closest to your current challenge, then use the working session to turn the guidance into a clear next action.

Map information before writing rules

Employee information travels through recruitment, payroll, management, support and exit processes. List the records used at each stage and the purpose they serve. Include exports, shared folders, messaging tools and supplier systems, not only the main HR platform.

This guide supports policy planning. Applicable privacy laws, lawful bases, notices, rights, transfers and retention requirements depend on context and need specialist review. For UK organisations, start with the ICO employment information guidance.

Draft a clear handling standard

A policy core might say: “We collect and use worker information for defined purposes, limit access to people who need it for their responsibilities and keep records accurate and appropriately protected.” Turn that statement into named controls and actual responsibilities.

Explain which systems are approved, how errors are corrected and where people ask privacy questions. Do not assume employee consent is the appropriate basis for every use. Have the relevant reviewer establish the justification and required notices for each processing activity.

Control access and retention in practice

Give managers access to the information necessary for their role. Keep medical, payroll and investigation material within appropriate restricted processes. Review access when someone joins, moves or leaves, including access inherited through group membership.

Define retention by record type, purpose and applicable requirements. State what event starts the period and who performs deletion. Check exports, backups and supplier copies. A deletion setting in one application does not establish that every copy has been removed.

Worked example: an exported review file

Illustrative scenario: a manager exports review notes for preparation and saves them in a widely shared folder. The organisation’s response first contains access and follows the internal incident process. An authorised reviewer determines any further obligations.

The process improvement provides an approved preparation workspace, clear export rules and a review of permissions. Training uses the scenario without exposing the employees in the

original records. The organisation checks whether the change works instead of relying only on a reminder email.

Data-handling worksheet

- **Record and purpose:** What information is needed, and why?
- **Source and owner:** Where does it come from, and who is accountable?
- **Access:** Which roles may view, edit, export or share it?
- **Suppliers and locations:** Who else processes it and under what reviewed arrangement?
- **Retention:** What rule applies, what starts it and how is deletion verified?
- **Employee route:** How can a person raise a question or exercise applicable rights?
- **Incident route:** Who receives a suspected loss, misuse or disclosure?

Complete the worksheet for one high-use record before expanding the inventory. Keep the resulting register controlled; it may itself describe sensitive systems or access arrangements.

Test the policy with real workflows

Check a starter, a manager change, an export, an access correction and an employee departure using approved test records. Verify that the expected permissions and deletion steps occur.

Review the policy before adding a new AI tool or data connection. Reusing information for a new purpose needs evaluation; existing access to a record does not automatically justify every new analysis of it.

Put the guide into practice

Set aside a working session with the people who own this process and one or two people who experience it. Use a fictional or appropriately authorised case, so the discussion can be specific without sharing unnecessary personal information. The purpose is to leave with a usable decision or document, not just agreement that the topic matters.

Prepare the case

Choose one record type, such as review notes, and trace its journey from creation to deletion. Include copies in email, exports and supplier systems. List the people who can access it and the purpose of each access. Ask whether the record contains information that belongs in a more restricted process.

Write the starting assumptions down before discussing solutions. If the group disagrees on what happened, identify the information needed to resolve that difference rather than building

a plan on an untested story.

Work through the decision

Define the approved handling route with the relevant privacy and security owners. Specify which system holds the authoritative record, who can correct it and which roles may export it. Check the proposed purpose and notices rather than assuming that an existing record can be reused for any convenient analysis.

Ask each participant to explain the proposed decision in their own words. Differences in interpretation often reveal an unclear criterion, a missing responsibility or an instruction that will be difficult to follow.

Test an exception

Simulate a manager transfer and an accidental export to the wrong folder using test data. Verify who loses access, who gains it and how a suspected disclosure is reported. The response should follow an established incident route; employees should not make their own legal notification decision or quietly delete evidence.

Record what changes in this situation and what remains the same. An exception should lead to a clear next step, with an owner, rather than an informal workaround that nobody can explain later.

Agree the handoff

Give the record owner a documented access and retention arrangement, including downstream copies. Confirm who performs periodic checks and who answers employee questions. A retention period without a deletion owner and an operational trigger is an intention rather than a complete process.

Finish by confirming the owner, the next action and the date when the result will be reviewed. Give the person receiving the work enough context to continue without repeating the whole discussion.

Frequently asked questions

Can HR keep information indefinitely just in case?

Retention should follow a defined purpose, applicable requirements and the organisation’s reviewed schedule. Keeping everything because it might be useful increases exposure and makes records harder to manage. Different record types may need different rules. Establish the relevant trigger, responsible owner and deletion or review process with appropriate specialists, including how legal holds or other exceptions are handled.

Does removing names make employee data anonymous?

Not necessarily. A job title, unusual event, small team or combination of details may still identify a person. Assess the information in context and consider what recipients already know. Use appropriate minimisation, access controls and reporting rules. If the proposed use depends on a claim of anonymity, have that claim reviewed rather than relying on a simple name-removal step.

Who should see a performance review record?

Access should reflect a legitimate role and the organisation’s approved process. The employee, relevant manager and authorised HR staff may have different needs, while sensitive supporting information may need tighter restrictions. Review access when roles change and explain it to participants. Do not assume every senior manager or project contributor needs the full record simply because they have organisational responsibility.

Review the first cycle

Verify a sample of actual permissions and deletion steps against the documented rules. Review where users create uncontrolled copies because the approved workflow is difficult. Fix the workflow as well as the instruction. Record unresolved gaps with owners and follow the appropriate incident process when a check reveals a possible disclosure.

Keep a brief record of what was tried, what participants found useful and what needs to change. Compare the result with the original problem rather than judging success only by completion. If the process created extra work without improving clarity, quality or support, simplify it and test again. Share the agreed change with the people who will use it, and name the person responsible for keeping the guidance current.

About New Dynamics

New Dynamics connects goals, feedback, recognition and reviews around the way organisations work. This guide is published by the New Dynamics Editorial Team as part of our practical library for HR leaders, managers and People teams.

Use the examples and worksheets to structure your own discussions and adapt them to your organisation. Illustrative scenarios are not customer case studies. Policy and employment guidance needs appropriate local review before adoption.

For questions about this guide, corrections or a conversation about your performance management process, email contact@new-dynamics.com. Explore the complete guide library for related resources.

Your working worksheet

Use the prompts from this guide to prepare one real conversation or decision. Keep personal or sensitive information in your organisation’s approved records. This page is for your own working notes.

Record and purpose: What information is needed, and why?

Source and owner: Where does it come from, and who is accountable?

Access: Which roles may view, edit, export or share it?

Suppliers and locations: Who else processes it and under what reviewed arrangement?

Retention: What rule applies, what starts it and how is deletion verified?

Employee route: How can a person raise a question or exercise applicable rights?

Incident route: Who receives a suspected loss, misuse or disclosure?

Discuss your next step with New Dynamics: contact@new-dynamics.com