Data Protection Impact Assessment (DPIA)

AI Productivity Programme — Microsoft Copilot & Claude (MCP Connectors)

Organisation: Example Consulting Ltd (50 employees) · **Prepared by:** @Mike · **Date:** 7 Oct 2026

Step 1: Identify the Need for a DPIA

A Data Protection Impact Assessment is required under Article 35 UK GDPR and ICO guidance because the project meets several of the ICO's screening criteria before any processing begins.

Screening outcome

Screening question (ICO DPIA screening checklist)	Applies?	Basis
Does the project use new technology, or apply existing technology in a novel way?	Yes	Generative AI assistants reading across live business systems via MCP connectors is a new processing method for this organisation
Does the processing involve evaluation or scoring of individuals, including profiling?	Partially	Copilot/Claude-generated meeting summaries and performance-related document drafting could indirectly profile staff if outputs are used in appraisals
Is there systematic monitoring of individuals?	Yes	Meeting transcription and summarisation captures employee contributions on an ongoing basis
Does the processing involve sensitive data or data of a highly personal nature?	Possibly	Email and document stores may incidentally contain special category data (health references in HR correspondence, trade union communications)
Is data processed on a large scale?	Yes	All 50 employees, the full customer and supplier contact base, and historic email/document archives are in scope
Does the processing involve matching or combining datasets from different sources?	Yes	Claude's MCP connectors combine SharePoint, CRM and knowledge-base content within a single session
Does the processing involve data transferred outside the UK?	Yes	Both vendors process data on US-domiciled infrastructure
Is it likely to result in a high risk to the rights and freedoms of individuals if controls fail?	Yes	Over-broad AI access or prompt leakage could expose personal data from several systems simultaneously

Because the project meets more than one screening criterion, a DPIA is mandatory, not merely good practice. This assessment is being completed **before** production deployment, in line with Article 35(1).

Trigger for this assessment: Board approval to pilot Microsoft Copilot (M365) and Claude Desktop with MCP connectors across the Operations and Customer Success teams, with a view to wider rollout after a 90-day pilot.

Step 2: Describe the Processing

Nature of the processing

Microsoft Copilot operates inside Outlook, Teams, Word, Excel and PowerPoint, drafting content, summarising meetings and answering questions against the user's existing M365 permissions. Claude Desktop connects to internal systems through Model Context Protocol (MCP) connectors — approved, scoped integrations that let Claude read (and in limited cases write to) named systems on the user's behalf, within that user's existing access rights. Neither tool is given standing access beyond what the individual user already holds; both are session-based and inherit, rather than expand, existing permissions.

Scope: systems and data in scope

System	Connected via	Data accessible	Read/write
Outlook / Exchange Online	Copilot (native)	Employee and customer email content, calendars	Read; draft replies (not auto-sent)
Teams	Copilot (native)	Meeting audio/transcripts, chat history	Read; summarise
SharePoint / OneDrive	Claude MCP connector	Contracts, HR documents, project files, financial records	Read only (pilot phase)
CRM (HubSpot)	Claude MCP connector	Customer contact details, deal notes, communication history	Read only (pilot phase)
Internal knowledge base (Confluence)	Claude MCP connector	Policies, process documentation, project retrospectives	Read only

No connector in this phase has been granted write access to source systems; Claude and Copilot outputs are reviewed and manually actioned by the employee.

Categories of data subjects

- Employees (all 50 staff, where email, Teams or HR-adjacent documents are accessed)
- Job applicants (where recruitment correspondence sits in mailboxes in scope)
- Customers and prospects (CRM and email correspondence)
- Suppliers and subcontractors (contract and correspondence records)

Categories of personal data

- Contact details (names, emails, phone numbers)
- Employment records referenced in HR correspondence (contracts, absence, disciplinary notes where these exist in mailboxes or SharePoint)
- Meeting content and transcripts, which may include opinions, performance discussion or informal remarks about third parties
- Customer and supplier commercial data (pricing, contract terms, deal history)
- Special category data risk: health information (e.g. occupational health emails), trade union or representative communications, and similarly sensitive content may be present incidentally within mailboxes and SharePoint, even though it is not a deliberate target of processing

Purposes of processing

To improve staff productivity through AI-assisted drafting, document retrieval, meeting summarisation and knowledge search, reducing time spent on repetitive information-gathering tasks.

Context

This is a new processing activity for the organisation. Staff have not previously had AI tools with this breadth of system access; the organisational and cultural context (first deployment of generative AI at this scale) is itself a risk factor, independent of the technical controls in place.

Volumes and retention

Approximately 50 employee mailboxes, an estimated 1,200 active CRM contact records and circa 15,000 SharePoint documents are within scope. Claude and Copilot do not create a persistent copy of source data; retrieved content is used within the session and is not stored by the AI vendor beyond the active session, per the data processing terms agreed with each vendor (see Appendix B). Prompts and outputs within Claude are retained in line with the organisation's existing M365/Claude workspace retention policy (90 days), not indefinitely.

Processors and sub-processors

Microsoft (Copilot, M365) and Anthropic (Claude) act as processors under data processing agreements already in place for the underlying M365 and Claude Enterprise subscriptions. Both vendors' sub-processor lists have been reviewed; no sub-processor introduces processing outside the UK/EU/US adequacy or SCC framework currently relied upon (see International Transfers, Step 4).

Step 3: Consultation Process

Stakeholder	Role in consultation	Date	Key input

Data Protection Officer	Led the DPIA, reviewed lawful basis and risk register	Ongoing	Required the legitimate interests assessment (LIA) to be documented separately and referenced here; required write access to be excluded from the pilot
IT Manager	Provided technical detail on connector scope, access controls and logging	Week 1	Confirmed MCP connectors can be scoped to read-only and restricted by SharePoint site/library, reducing access to the minimum needed
Employee representatives (2, nominated informally from Operations and Customer Success)	Represented staff concerns about AI reading personal correspondence and meeting content	Week 2	Raised concern about Teams meeting summarisation capturing informal remarks; resulted in an opt-out being added for sensitive meetings and a staff notice being issued before go-live
HR Lead	Assessed exposure of employment and health-adjacent records	Week 2	Recommended HR's dedicated SharePoint library be excluded from the connector scope entirely during the pilot
External legal adviser	Reviewed vendor contracts and international transfer mechanisms	Week 3	Confirmed Microsoft's and Anthropic's standard contractual clauses meet UK GDPR Article 46 requirements; flagged a gap in Anthropic's sub-processor list requiring written clarification

No wider staff survey or works council consultation was undertaken, as the organisation has no works council and the pilot is limited to two departments by headcount (18 of 50 staff) in its first phase. Should the DPIA risk assessment support organisation-wide rollout, a full staff briefing and Q&A session is planned before Phase 2 (see Step 7).

Feedback from this consultation directly shaped the project: HR records were removed from scope, a meeting opt-out was introduced, and the legal gap on Anthropic's sub-processor list was escalated and closed before this DPIA could proceed to sign-off (see Appendix B for the closure evidence).

Step 4: Assess Necessity and Proportionality

Lawful basis: Legitimate Interests (Article 6(1)(f))

A three-part Legitimate Interests Assessment (LIA) was completed and is held as a supporting document; its conclusions are summarised here.

Purpose test: The organisation has a genuine business interest in improving staff productivity, reducing time spent on manual document retrieval and administrative drafting, and building institutional knowledge continuity. This is a real and current interest, not speculative.

Necessity test: The processing is necessary to achieve that purpose. A non-AI alternative (manual search, existing search tools) was considered and rejected as insufficient to achieve the productivity and knowledge-retrieval gains sought; however, necessity does not extend to write access, broad/unscoped connector permissions, or indefinite retention of prompts, all of which have been excluded or time-limited accordingly.

Balancing test: Employees, customers and suppliers have a reasonable expectation that their business correspondence may be processed by productivity tooling, particularly where this mirrors existing use of M365 search and Teams transcription (already in use). The balancing test identifies two groups requiring extra weight: (1) employees, whose correspondence and meeting contributions carry a higher expectation of privacy than customer-facing data, addressed through the meeting opt-out and HR exclusion; and (2) any data subject whose personal data happens to include special category information, addressed by excluding HR's SharePoint library and by instructing staff not to reference health, union or similarly sensitive matters inside AI-assisted drafting. On balance, the organisation's interest is not overridden by the interests or fundamental rights of data subjects, **provided** the mitigations identified in this DPIA are implemented.

Data minimisation

Access is scoped per connector rather than granted globally: Claude's SharePoint connector is restricted to specific document libraries (Operations, Customer Success, Knowledge Base), explicitly excluding the HR library. CRM access is limited to the fields required for customer service and account management, excluding internal credit-risk notes. Copilot inherits the user's own M365 permissions and cannot access mailboxes or files the user could not already open directly — no new access is created, only a new way of querying existing access.

Could the purpose be achieved another way?

A lower-risk alternative — restricting AI tools to a single, curated knowledge base rather than live connectors into SharePoint, CRM and email — was considered. This was rejected for the pilot's goals (reducing time spent switching between live systems) but remains available as a fallback if the pilot identifies risks that cannot be adequately controlled.

Retention

Prompts, outputs and session logs are retained for 90 days in line with the organisation's existing M365 and Claude Enterprise retention settings, then automatically deleted. This mirrors the organisation's existing retention schedule for Teams chat and is not an extension of retention beyond current practice.

Individual rights

The organisation's existing privacy notice and data subject rights procedures (subject access, erasure, objection) apply unchanged to any personal data processed through Copilot or Claude,

since no new category of processing purpose is created — only a new tool operating within existing purposes. The privacy notice has been updated to specifically name AI-assisted processing as a use case, and this update was issued to staff and published externally before pilot go-live.

Step 5: Identify and Assess Risks

Methodology: Likelihood and impact are each scored 1 (low) to 5 (high); Score = Likelihood × Impact. Low: 1–6, Medium: 7–14, High: 15–25. Residual risk is the score expected after the controls in Step 6 are implemented and operating effectively.

#	Risk	Likelihood	Impact	Score	Key controls	Owner	Residual
1	Excessive access via MCP connector (connector scoped too broadly, exposing HR, financial or special category data beyond what the use case requires)	3	5	15 (High)	Role-based access control; least-privilege connector scoping by library/field; documented approval process for any new connector or scope change	IT Manager	Medium
2	Staff enter sensitive or excessive personal data into prompts (e.g. pasting a customer's health details or a colleague's disciplinary record into a Claude or Copilot prompt)	3	4	12 (Medium)	Staff AI acceptable-use policy; mandatory training before access is granted; DLP rules flagging special-category keywords in prompts	DPO	Low
3	AI hallucination or factual error is relied upon without review (e.g. a fabricated contract term or incorrect customer detail is acted on)	3	3	9 (Medium)	Mandatory human validation before any AI output affecting an individual's rights, a contract or a customer communication is sent or acted on	Department Managers	Low

4	Misconfigured connector permissions (a technical fault or admin error grants broader access than intended, e.g. to the HR library)	2	5	10 (Medium)	Security review and penetration-style testing of each connector before go-live; quarterly access recertification; configuration changes require a second approver	IT Manager	Low
5	Data breach or unauthorised access at the vendor (Microsoft or Anthropic infrastructure is compromised, or vendor staff access UK personal data inappropriately)	2	5	10 (Medium)	Vendor due diligence completed; DPAs and SCCs in place; encryption in transit and at rest confirmed; vendor breach-notification clause (72-hour notice) contractually required	DPO	Low
6	Re-identification or profiling of employees through aggregated AI usage logs (e.g. meeting summaries or query history reveal performance patterns used informally in appraisals)	2	4	8 (Medium)	Usage logs restricted to IT/security purposes only; explicit policy that AI usage data must not be used in performance management; employee opt-out for sensitive meetings	HR Lead	Low
7	International transfer of personal data without adequate safeguards (vendor processing occurs on US	2	4	8 (Medium)	Standard Contractual Clauses executed with both vendors; transfer risk assessment (TRA) completed and	DPO	Low

	infrastructure outside UK adequacy)				reviewed by external legal adviser		
8	Function creep: pilot scope expands informally (e.g. staff connect additional systems or extend write access without re-assessment)	3	3	9 (Medium)	Change control requiring DPIA addendum for any new connector, new data source, or move from read-only to write access	IT Manager	Low

Highest residual concern: Risk 1 (excessive access via connector) remains Medium even after controls, because connector scoping is a configuration setting rather than a structural limit — human error in reconfiguration remains possible. This is the risk the Step 7 sign-off conditions focus on most closely.

Step 6: Identify Measures to Reduce Risk

Control	Mitigates risk #	Type	Owner	Target date	Status
Scope all MCP connectors to read-only for the pilot; no write-back to SharePoint, CRM or email	1, 8	Technical	IT Manager	Complete	Implemented
Exclude HR SharePoint library from connector scope entirely	1, 6	Technical	IT Manager	Complete	Implemented
Connector access approval workflow: any new connector, data source or scope change requires DPO and IT Manager sign-off	1, 8	Organisational	IT Manager	Before Phase 2	In progress
AI acceptable-use policy issued to all pilot staff, covering what must not be entered into prompts	2	Organisational	DPO	Complete	Implemented
Mandatory 30-minute AI awareness training before connector access is granted	2, 3	Organisational	HR Lead	Complete (pilot cohort); ongoing	Implemented

				for new joiners	
DLP keyword rules flagging likely special-category content in prompts (health, union, religion-related terms)	2	Technical	IT Manager	Within 30 days of pilot start	In progress
Human-in-the-loop requirement: no AI-drafted content affecting an individual's rights, a contract, or external communication is sent without manual review	3	Organisational	Department Managers	Complete	Implemented
Independent security review and configuration test of each connector before go-live	4	Technical	IT Manager	Complete	Implemented
Quarterly access recertification of all connector scopes	1, 4	Organisational	IT Manager	First review: Q1 2027	Scheduled
Vendor due diligence pack (security certifications, DPA, sub-processor list) reviewed and filed	5	Organisational	DPO	Complete	Implemented
Standard Contractual Clauses executed with Microsoft and Anthropic; Transfer Risk Assessment completed	5, 7	Legal	DPO	Complete	Implemented
Usage-log access restricted to IT/security; written policy that logs must not inform performance management	6	Organisational	HR Lead	Complete	Implemented
Opt-out mechanism for staff to exclude specific meetings from AI transcription/summarisation	6	Technical	IT Manager	Complete	Implemented
Change control: any scope expansion (new connector, new data source, read-only to write) triggers a DPIA	8	Organisational	DPO	Complete (process defined)	Implemented

addendum before implementation

All controls above were either implemented before this DPIA's sign-off or have a committed target date; none is contingent on this assessment being approved first — the organisation is not relying on future controls to justify current risk acceptance.

Step 7: Sign-off and Outcomes

DPO opinion: The processing is lawful, necessary and proportionate, provided the controls in Step 6 remain in place and the conditions below are met. The DPO's view is that residual risk is acceptable for a limited, read-only pilot across two departments, but would need to be reassessed before any organisation-wide rollout or any move to write access.

Overall residual risk rating: Medium, driven by Risk 1 (connector over-scoping). This is a lower rating than the initial assessment (High, before controls), reflecting the exclusions, approval workflow and technical scoping already implemented.

Decision: Approved to proceed to pilot, subject to the following conditions:

1. The pilot remains read-only across all connectors; no write access is enabled without a DPIA addendum.
2. HR's SharePoint library remains excluded from connector scope for the duration of the pilot.
3. The DLP keyword rules (Step 6) are live before any staff outside the original pilot cohort are granted access.
4. A pilot review takes place at 90 days, covering: any incidents or near-misses, actual usage patterns against the access granted, and staff feedback from the consultation group.
5. This DPIA is reassessed in full — not simply refreshed — before any decision to extend to additional departments, add write access, or connect additional systems.

Review date: 8 January 2027 (90 days from pilot start), or earlier if a notifiable incident occurs or scope changes.

Approvals

Name	Role	Decision	Date
[DPO name]	Data Protection Officer	Approved, subject to conditions above	7 October 2026
[IT Director/Manager name]	IT Manager	Approved	7 October 2026
[Managing Director name]	Senior management sponsor	Approved	7 October 2026

If the DPO's advice above were to be overridden by management, that decision and its reasons would be recorded here — no such override applies to this assessment.

Appendix A: Data Flow (Description)

1. A pilot user opens Microsoft Copilot or Claude Desktop and enters a prompt relating to their work (e.g. drafting a client update, summarising a document).
2. Where the prompt or an attached MCP connector requires data beyond the model's own training, the relevant connector (SharePoint, CRM, or knowledge base) is queried, scoped to that user's existing permissions — the connector does not expose data the user could not already access directly.
3. Retrieved content is passed to the AI model (Microsoft-hosted for Copilot; Anthropic-hosted for Claude) together with the prompt, processed, and a response returned to the user's session.
4. Prompts, retrieved context and responses are not used to train the underlying models (per the vendor terms reviewed in Step 2) and are retained only per each vendor's standard operational retention period.
5. No data flows from either vendor into the other; each sits in its own isolated processing path from the same underlying source systems.
6. HR's SharePoint library is excluded from connector scope at the permissions layer, so no HR content enters this flow regardless of user permissions elsewhere.

Appendix B: MCP Connector Permissions Inventory

Connector	Source system	Scope granted	Excluded content	Access model	Reviewed by
SharePoint connector	Operations SharePoint site	Read-only, sites the pilot user already has access to	HR document library (explicitly excluded)	Inherits user's existing M365 permissions	IT Manager
CRM connector	Customer Success CRM	Read-only, records assigned to or shared with the pilot user	Billing/finance module	Inherits user's existing CRM role	IT Manager
Knowledge base connector	Internal knowledge base	Read-only, published pages only	Draft/unpublished pages	Inherits user's existing KB role	IT Manager

	(Confluence-style)				
Calendar/meeting context	M365 Calendar	Read-only, pilot user's own calendar	Meetings marked private; any attendee who opted out	Opt-in per pilot user, opt-out honoured per attendee	HR Lead

All connector permissions are reviewed at the 90-day pilot review (Step 7) and before any extension of scope.

Appendix C: Review and Monitoring Schedule

Trigger	Review	Owner	Due
Routine	90-day pilot review (usage, incidents, feedback)	IT Manager + DPO	8 January 2027
Routine	DLP keyword rule effectiveness check	IT Manager	30 November 2026
Routine	Connector permissions re-review	IT Manager	8 January 2027
Event-driven	Any notifiable data breach involving pilot data	DPO	Within 72 hours of discovery
Event-driven	Request to extend pilot to new departments or enable write access	DPO	Before extension proceeds
Event-driven	Change to vendor sub-processor list or DPA terms	DPO	Within 30 days of notice
Annual	Full DPIA reassessment	DPO	October 2027, or earlier per triggers above