



Northwind Traders

PREPARED BY

Harbour IT

DATE

12 October 2026

EVIDENCE DATE

11 Oct 2026

SCHEME

ICO

MICROSOFT 365 TENANT

northwindtraders.onmicrosoft.com

● Gaps to close

Northwind Traders has 6 controls not in place.

IN THIS REPORT

Summary	2
Gaps to close	3
A. Manage security risk	4
B. Protect personal data against cyber-attack	6
C. Detect security events	13
D. Minimise the impact	14
Accountability records	16
About this evidence	17

Summary

Northwind Traders has 6 controls not in place.

How the client's Microsoft 365 meets the ICO's security outcomes for UK GDPR, with the accountability records a client, insurer or the ICO asks for. Use it for a client's data protection review, a DPIA or the questions after a breach.

18 controls need evidence Microsoft 365 can't show (firewalls, patch timing, anti-malware settings and processes): each has a text to complete.

29 controls



■ **2** Pass ■ **6** Fail ■ **3** Partly ■ **18** Your evidence

Gaps to close

The controls most likely to be queried, with the fix for each.

1 A.4 Processors and the supply chain

Users can consent to any app. Fix: Set user consent to "Allow user consent for apps from verified publishers, for selected permissions" or turn it off and use the admin consent workflow.

2 B.2 Identity and access: multi-factor authentication

Enforced by Require MFA for all users, with 1 exclusion to review. Fix: Create a Conditional Access policy requiring MFA for all users and all cloud apps, or turn on Security Defaults if the tenant has no Entra ID P1.

3 B.3 Data security: sharing

3 files and folders shared with anyone. Fix: Remove anyone links that are no longer needed, and set the rest to view-only with an expiry date.

4 B.3 Data security: encryption

4 of 36 computers not encrypted. Fix: Turn on BitLocker.

5 B.4 System security: updates and device management

5 of 36 Windows computers past end of support. Fix: Upgrade computers on Windows 10 or an old Windows 11 release to the current Windows 11 release.

6 C.1 Security monitoring: suspicious activity

1 suspicious inbox rule. Fix: Check each rule with the mailbox owner.

7 B.2 Identity and access: administrators

1 guest with admin roles. Fix: Remove admin roles from guest accounts.

8 B.2 Identity and access: leavers and shared accounts

4 accounts inactive for 90+ days or never used. Fix: Disable accounts that haven't signed in for 90 days, or were created over 30 days ago and never used.

9 B.3 Data security: email leaving the organisation

4 external forwards. Fix: Remove forwarding to outside addresses unless the client has a documented business reason.

A. Manage security risk

● Fail

Someone is accountable, risks to personal data are assessed, the data and systems are known, and processors are under contract.

A.1 Governance: accountable people and policies

● Your evidence

Senior management is accountable for the security of personal data, with named roles and policies.

Text to paste: [Name], [role], has overall responsibility for information security and data protection and reports to [the board or partners], where security is a standing agenda item. Day-to-day IT security is managed by [IT provider].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

A.1 Data protection officer or lead

● Your evidence

A Data Protection Officer is appointed where the law requires one; otherwise a named person leads.

Text to paste: [The organisation has appointed (name) as its Data Protection Officer, contactable at (email address).] or [The organisation assessed on (date) that it doesn't need a Data Protection Officer; (name, role) is responsible for data protection.]

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

A.2 Risk management

● Your evidence

Risks to personal data are assessed, recorded and treated, and the assessment is kept current.

Text to paste: An information security risk assessment covering [scope] names an owner for each risk, the agreed treatment and an action plan. It was last reviewed on [date] by [name and role] and approved by [director or partner].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

A.3 Asset management

● Your evidence

The systems and devices that hold personal data are known, with owners.

WHAT WE FOUND

- But: 1 of 39 device records unused for 90+ days.
- But: 1 of 37 joined computers not in Intune.
- Computers managed by Intune: 36
- Of which encrypted: 32
- Windows computers out of support: 5
- Reaching end of support within 90 days: 20
- Not compliant: 6

Text to paste: An asset register in [tool or spreadsheet] lists [hardware, software, cloud services and the information held], each with a named owner, a category and where it is. Devices are added when they're set up and removed when they're disposed of, and the register was last reviewed on [date].

What Microsoft 365 can't show: Microsoft 365 lists the devices Intune and Entra ID know; the register covers everything else.

A.4 Processors and the supply chain

● Fail

Processors are chosen for their security and bound by contract (Article 28), and the cloud apps that reach the data are controlled.

GAPS

- Users can consent to any app.
 - Any user can grant any app access to their mail and files
- 1 app with access to mail, files or the directory.
 - Mail Sync Pro: Mail.Read (application permission; unverified publisher)

Fix: Set user consent to "Allow user consent for apps from verified publishers, for selected permissions" or turn it off and use the admin consent workflow. Consent phishing relies on this setting.

Text to paste: Every supplier that processes personal data for the organisation has a written contract with the terms UK GDPR Article 28 requires: acting only on instructions, confidentiality, security, approval of sub-processors, help with people's rights, and deleting or returning the data at the end. They're recorded in [register].

What Microsoft 365 can't show: Microsoft 365 shows which apps can reach its data; the contracts are the organisation's own.

A.4 Where the data is held

● Pass

The organisation knows where personal data is stored, and transfers outside the UK have a lawful safeguard.

WHAT WE FOUND

- Email, files and Teams data are held in Microsoft 365, in Microsoft's datacentres.

What Microsoft 365 can't show: Judged from the tenant's country in Microsoft 365. Add other services that hold personal data.

B. Protect personal data against cyber-attack

● Fail

Policies are followed, access is by named accounts with MFA, data is encrypted and not shared openly, systems are updated and managed, and staff are trained.

B.1 Service protection policies and processes

● Your evidence

Policies and processes say how personal data and the systems that hold it are protected.

Text to paste: Information security policies covering [acceptable use, access control, passwords, data protection and incident response] are approved by [role], reviewed every [12 months] and acknowledged by staff.

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

B.2 Identity and access: multi-factor authentication

● Fail

Everyone who can reach personal data signs in with multi-factor authentication, and protocols that can't use it are blocked.

WHAT WE FOUND

- But: 14 users without MFA.
- But: 3 people can only use a text or call as a second factor.
- Users with an MFA method registered: 62.2% of 37
- Accounts covered by an enforced MFA policy: 36 of 36

GAPS

- Enforced by Require MFA for all users, with 1 exclusion to review.
 - breakglass@northwindtraders.example: Excluded from "Require MFA for all users"
- 1 admin not covered by MFA.
 - breakglass@northwindtraders.example: Global Administrator: excluded from Require MFA for all users
- Legacy authentication is allowed.
 - No enabled policy blocks legacy authentication for all users

Fix: Create a Conditional Access policy requiring MFA for all users and all cloud apps, or turn on Security Defaults if the tenant has no Entra ID P1. Keep exclusions to break-glass accounts.

Text to paste: Multi-factor authentication (MFA) is enforced for Microsoft 365 email (including Outlook on the web and mobile) and cloud applications, through Microsoft Entra ID. Enforced by Conditional Access ("Require MFA for all users") for everyone except 1 named exclusion: breakglass@northwindtraders.example (break-glass).

What Microsoft 365 can't show: Judged for Microsoft 365 sign-ins. Add other systems that hold personal data.

B.2 Identity and access: administrators

● Partly

Administrator access is limited to named people who need it.

WHAT WE FOUND

- 2 Global Administrators.
- Accounts holding privileged roles: 4
- Admins with no MFA policy: 1
- Admins with no MFA method registered: 2

GAPS

- 1 guest with admin roles.
 - g#EXT#@northwindtraders.example: Guest holding Exchange Administrator
- 1 app with privileged roles.
 - Some app: App holding Exchange Administrator

Fix: Remove admin roles from guest accounts. If an external partner needs access, use GDAP or a member account in this tenant protected by MFA.

Text to paste: Administrator role assignments in Microsoft 365 are tracked, with gaps. 4 accounts hold privileged admin roles, 2 of them Global Administrator (ann.patel@northwindtraders.example, breakglass@northwindtraders.example). 2 Global Administrators. 1 guest with admin roles. 1 app with privileged roles.

What Microsoft 365 can't show: Judged from Microsoft 365 and Entra ID admin roles.

B.2 Identity and access: leavers and shared accounts

● Partly

Access ends when people leave, and every sign-in belongs to a person.

WHAT WE FOUND

- All 3 shared mailboxes block sign-in.

GAPS

- 4 accounts inactive for 90+ days or never used.
 - hannah.robinson@northwindtraders.example: Licensed member, last signed in 7 Apr 2026
 - sophie.smith@northwindtraders.example: Licensed member, last signed in 21 Jan 2026
 - thomas.clarke@northwindtraders.example: Licensed member, last signed in 2 Jun 2026
 - g#EXT#@northwindtraders.example: Guest, never signed in, created ?
- 1 disabled account still licensed.
 - robert.hughes@northwindtraders.example: Disabled, holding 1 licence

Fix: Disable accounts that haven't signed in for 90 days, or were created over 30 days ago and never used (after checking with the client), then remove their licences. Inactive accounts are a common foothold for attackers.

Text to paste: Some inactive accounts in Microsoft Entra ID have not been disabled. 4 accounts inactive for 90+ days or never used. 1 disabled account still licensed.

What Microsoft 365 can't show: Judged from Entra ID accounts, sign-in activity and shared mailboxes.

B.3 Data security: sharing

● Fail

Personal data isn't open to anyone with a link, and guests are controlled.

GAPS

- 3 files and folders shared with anyone.
 - Campaign video.mp4 (Marketing / Documents): Anyone can edit
 - Brand assets (Marketing / Documents): Anyone can view, link never expires
 - holiday.jpg (OneDrive of ann.patel@northwindtraders.example): Anyone can view
- Anyone, including anonymous links.
 - SharePoint and OneDrive: Anyone links are allowed
- Anyone, including guests, can invite guests.
 - Guests can invite other guests

Fix: Remove anyone links that are no longer needed, and set the rest to view-only with an expiry date. The Shared files report lists each one.

Text to paste: Sharing with anonymous and external users is not restricted in SharePoint and OneDrive. Anyone, including anonymous links. 3 files and folders shared with anyone. Anyone, including guests, can invite guests.

What Microsoft 365 can't show: Judged from SharePoint and OneDrive sharing settings and links.

B.3 Data security: email leaving the organisation

● Partly

Mail isn't forwarded outside unnoticed, and the domains can't be spoofed to trick people into sending data.

WHAT WE FOUND

- The default outbound policy blocks automatic external forwarding.
- But: 1 domain with SPF problems.
- But: 1 mail domain without DKIM.
- But: 1 of 1 mail domain doesn't fully enforce MTA-STS.

GAPS

- 4 external forwards.
 - ann.patel@northwindtraders.example: Mailbox forwarding to ann.patel@homemail.example (keeps a copy)
 - ann.patel@northwindtraders.example: Inbox rule "Copy to home" forwards to ann.patel.home@homemail.example
 - grace.taylor@northwindtraders.example: Mailbox forwarding to grace.taylor@homemail.example (doesn't keep a copy)
 - olivia.smith@northwindtraders.example: Inbox rule "Invoices to bookkeeper" forwards to bookkeeping@ledgerline.example
- 2 domains without DMARC enforcement.
 - northwindtraders.example: DMARC is monitor-only (p=none); spoofed mail is still delivered
 - parked.example: Doesn't receive mail but has no DMARC p=reject record

Fix: Remove forwarding to outside addresses unless the client has a documented business reason. Forwarding is the most common way attackers keep reading a mailbox after a password reset.

Text to paste: Automatic forwarding to external addresses is restricted in Exchange Online, with exceptions. The default outbound policy blocks automatic external forwarding. But 4 external forwards found.

What Microsoft 365 can't show: Judged from Exchange Online forwarding settings and public DNS.

B.3 Data security: encryption

● Fail

Personal data is encrypted on laptops and other devices that could be lost, and in transit.

WHAT WE FOUND

- But: 1 of 1 mail domain doesn't fully enforce MTA-STS.

GAPS

- 4 of 36 computers not encrypted.
 - DESK-WRIGHT18
(leo.wright@northwindtraders.example):
Windows disk isn't encrypted
 - LAPTOP-HUGHES
(robert.hughes@northwindtraders.example):
Windows disk isn't encrypted
 - LAPTOP-SCOTT29
(olivia.scott@northwindtraders.example):
Windows disk isn't encrypted
 - LAPTOP-SMITH07
(olivia.smith@northwindtraders.example):
Windows disk isn't encrypted

Fix: Turn on BitLocker (Windows) and FileVault (macOS) with an Intune disk encryption policy, with recovery keys escrowed to Entra ID, so a lost or stolen laptop doesn't expose the client's data.

Text to paste: Data in Microsoft 365 is encrypted at rest by Microsoft (BitLocker and per-file service encryption) and in transit using TLS. Not every company computer is encrypted: 4 of 36 computers not encrypted.

What Microsoft 365 can't show: Judged from Intune for company computers; Microsoft encrypts Microsoft 365 data itself.

B.4 System security: updates and device management

● Fail

Devices are managed and supported by their vendor, and security updates are installed promptly.

WHAT WE FOUND

- Computers managed by Intune: 36
- Of which encrypted: 32
- Windows computers out of support: 5
- Reaching end of support within 90 days: 20
- Not compliant: 6

GAPS

- 5 of 36 Windows computers past end of support.
 - LAPTOP-HUGHES
(robert.hughes@northwindtraders.example):
Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-MARTIN22
(maya.martin@northwindtraders.example):
Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-PATEL13
(hannah.patel@northwindtraders.example):
Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-ROBERTS31
(george.roberts@northwindtraders.example):
Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - LAPTOP-TAYLOR04
(grace.taylor@northwindtraders.example):
Windows 10 stopped getting security updates on 14 Oct 2025. Extended Security Updates or LTSC can cover it; otherwise upgrade.
 - and 20 more
- 6 of 37 managed devices not compliant.
 - DESK-ROBINSON12
(george.robinson@northwindtraders.example):
Not compliant
 - DESK-WRIGHT18
(leo.wright@northwindtraders.example): Not compliant
 - LAPTOP-HUGHES
(robert.hughes@northwindtraders.example): Not compliant
 - LAPTOP-SCOTT25
(alfie.scott@northwindtraders.example): Not compliant
 - LAPTOP-SCOTT29
(olivia.scott@northwindtraders.example): Not compliant
 - and 1 more
- 1 of 37 joined computers not in Intune.
 - DESK-RECEPTION: Hybrid joined, not managed by Intune

Fix: Upgrade computers on Windows 10 or an old Windows 11 release to the current Windows 11 release (Intune: Windows feature updates policy). Replace hardware that can't run Windows 11, or buy Extended Security Updates as a stopgap.

Text to paste: Managed Windows computers run versions of Windows that no longer receive security updates. 5 of 36 Windows computers past end of support.

What Microsoft 365 can't show: Judged from Intune. Add servers and devices it doesn't manage.

B.4 System security: malware protection

● Your evidence

Every device is protected from malware.

Text to paste: All desktops and laptops run [anti-malware product, for example Microsoft Defender Antivirus], which updates automatically, scans files when they're opened and blocks malicious websites. Tablets and phones only install apps from the official app stores.

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

B.5 Staff awareness and training

● Your evidence

Staff are trained to handle personal data securely and to spot phishing.

Text to paste: All staff complete security awareness training [when they join and every year], through [training provider or platform]. Simulated phishing exercises run [monthly or quarterly] and the results are reviewed by [role].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

C. Detect security events

● Fail

Activity is logged, suspicious sign-ins and mailbox rules are caught, and someone looks.

C.1 Security monitoring: logging

● Pass

Access to personal data and administrator actions are logged.

WHAT WE FOUND

- Mailbox auditing is on for the organisation.

Text to paste: Mailbox audit logging is enabled in Exchange Online, recording access to and actions on mailboxes. Mailbox auditing is on for the organisation.

What Microsoft 365 can't show: Judged from Exchange Online mailbox auditing and the unified audit log.

C.1 Security monitoring: suspicious activity

● Fail

Suspicious sign-ins, risky accounts and mailbox rules that hide or forward mail are detected.

WHAT WE FOUND

- Not checked: no accounts are at risk in Entra ID Protection (Risky users need Entra ID P2).
- Not checked: no risky sign-ins succeeded (Sign-in risk needs Entra ID P2).

GAPS

- 1 suspicious inbox rule.
 - ann.patel@northwindtraders.example: ".": Moves to RSS Feeds mail mentioning invoice, payment; Rule name '!' looks deliberately blank

Fix: Check each rule with the mailbox owner. Rules that delete or bury messages about payments or security alerts are a sign of a compromised account: reset the password, revoke sessions and review sign-ins.

Text to paste: Sign-ins are monitored for suspicious activity by [tool or service], and alerts are reviewed by [team or provider] [within one working day].

What Microsoft 365 can't show: Judged from Entra ID Protection and inbox rules (Entra ID P2 for the full detections).

C.1 Security monitoring: alerts reviewed

● Your evidence

Alerts and logs are reviewed by someone who can act on them.

Text to paste: Security alerts and sign-in logs are reviewed [daily or weekly] by [team or provider]. Logs are kept for [period] where users can't change them.

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

D. Minimise the impact

● Your evidence

Incidents are handled to a plan, breaches go to the ICO within 72 hours when required, data can be restored, and lessons are learned.

D.1 Response and recovery planning

● Your evidence

There is a plan for responding to incidents, including containing a compromised account.

Text to paste: A documented incident response plan sets out roles, contacts and the steps to contain and recover from a cyber incident, including notifying [the insurer and IT provider]. It was last reviewed on [date] and tested on [date].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

D.1 Breach reporting within 72 hours

● Your evidence

Personal data breaches are recorded, reported to the ICO within 72 hours of becoming aware when they're reportable, and the people affected are told when the risk to them is high (Articles 33 and 34).

Text to paste: Every personal data breach is recorded in a breach log with what happened, its effects and what was done. [Role] decides whether it must be reported; reportable breaches go to the ICO within 72 hours of the organisation becoming aware, and to the people affected when the risk to them is high. Lessons learned are reviewed by [role].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

D.1 Restoring personal data

● Your evidence

Personal data can be restored promptly after an incident, from backups that are tested.

Text to paste: Microsoft 365 data (Exchange Online mail, OneDrive, SharePoint and Teams) is backed up [daily] by [backup product or provider] to storage separate from Microsoft 365. Backups are kept for [retention period], are [immutable or offline], and use credentials separate from the Microsoft 365 administrator accounts. Restores were last tested on [date].

What Microsoft 365 can't show: Microsoft 365 doesn't back itself up for this purpose; describe the backup of Microsoft 365 too.

D.2 Improvements: measures tested regularly

● Your evidence

The security measures are tested and assessed regularly (Article 32(1)(d)), for example by vulnerability scans, and lessons from incidents and tests are acted on.

Text to paste: External vulnerability scans run [monthly] using [tool or provider]. [A penetration test was last carried out on (date) by (provider).]

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

Accountability records

● Your evidence

What a client, an insurer or the ICO asks to see after a breach: the record of processing, the privacy notice, rights requests, impact assessments, retention and the ICO fee.

Art. 30 Record of processing activities

● Your evidence

A record of the personal data held, why, on what lawful basis, who it's shared with and how long it's kept.

Text to paste: A record of processing activities lists each kind of personal data held, its purpose and lawful basis, who it's shared with, where it's stored and how long it's kept. [Role] maintains it, and it was last reviewed on [date].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

Art. 13 and 14 Privacy notice

● Your evidence

People are told what's collected, why, how long it's kept, their rights and how to complain.

Text to paste: A privacy notice at [web address] explains what personal data is collected, why and on what lawful basis, who it's shared with, how long it's kept, people's rights and how to complain. It was last reviewed on [date].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

Art. 15 to 22 People's rights

● Your evidence

Requests to see, correct or delete personal data are answered within a month, and complaints handled.

Text to paste: Requests to see, correct or delete personal data, and complaints about how it's used, go to [contact] and are logged in [system]. They're answered within one month, and [role] checks each response before it's sent.

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

Art. 35 Data protection impact assessments

● Your evidence

An impact assessment is done before processing likely to be high risk to people.

Text to paste: A data protection impact assessment is carried out before any new system or process that is likely to be high risk to people, using [the ICO's template]. [Role] signs each one off, and the ICO would be consulted if a high risk remained.

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

Art. 5(1)(e) Kept no longer than needed

● Your evidence

Personal data is kept only as long as it's needed, then deleted.

Text to paste: A retention schedule sets how long each kind of data is kept. Data past its retention period is deleted [by Microsoft 365 retention policies or at a review every (period)], and the data held is reviewed [every 12 months] to check it's still needed.

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

ICO data protection fee

● Your evidence

The organisation has paid the data protection fee to the ICO, unless it's exempt.

Text to paste: The organisation is registered with the Information Commissioner's Office, registration number [ZA number], renewed on [date].

What Microsoft 365 can't show: All of this. Answer from the organisation's own records.

About this evidence

The ICO judges what was appropriate to the risk and the state of the art, so a gap here isn't automatically a breach of the law, but it's what the ICO would ask about after an incident.

Scope: personal data held outside Microsoft 365 (line-of-business systems, paper) needs the same measures. A Pass here covers Microsoft 365.

Requirements: UK GDPR Articles 5, 24, 28, 30, 32 to 35, and the ICO's security outcomes (A to D). The security outcomes are the ICO's, set out with the NCSC, and are under review after the Data (Use and Access) Act 2025; check the ICO's guide to data security for changes. The law and outcomes are paraphrased.

Prepared by Harbour IT (help@harbourit.example · 0161 496 0000). Pass and Fail are judged from Microsoft 365 settings and accounts read with read-only access; nothing was changed. The oldest data used was collected 11 Oct 2026, 20:31 UTC. Accepted risks are exceptions the organisation has reviewed and documented. Complete the [parts in brackets] before using a text.