Managed Services

GOVERNANCE & ASSURANCE

CONTROLLED COMPANY DOCUMENT

Privacy and Data Protection Policy

Practical controls for lawful, fair and secure handling of personal information.

Document owner: Max Pocock, Lead Consultant
Operational role: Data Protection Lead (not a statutory Data Protection Officer appointment)
Version: 1.0
Issued: 23 July 2026
Review due: 23 July 2027, or earlier after a material legal, contractual, service or processing change
Applies to: Managed Services Ltd, Max Pocock, and every separately engaged human specialist, subcontractor or supplier given access to personal information for company work

Managed Services Ltd handles personal information only for a defined and lawful purpose, limits access and use, protects it throughout its lifecycle, and remains accountable for decisions and incidents.

1. Purpose and status

This policy sets the minimum data-protection controls for Managed Services Ltd's business operations and client engagements. It applies whether the company acts as a controller, joint controller or processor. The role and responsibilities must be recorded for each material processing activity.

The policy is designed around the UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025 and, where relevant, the Privacy and Electronic Communications Regulations 2003. It must be read with the applicable contract, privacy notice, information-security requirements and client instructions. A stronger legal or contractual requirement takes priority.

This is an internal governance policy, not a privacy notice. People must receive clear privacy information relevant to the actual processing.

2. Data-protection principles

Managed Services Ltd applies the following principles to all personal information:

- **Lawfulness, fairness and transparency:** identify and record a lawful basis, use information in ways people can reasonably understand, and provide appropriate privacy information.
- **Purpose limitation:** collect information for specified, explicit and legitimate purposes and assess compatibility before any new use.
- **Data minimisation:** collect and retain only what is adequate, relevant and necessary.
- **Accuracy:** take reasonable steps to keep material information accurate and correct or delete inaccurate information without avoidable delay.

- **Storage limitation:** set and apply retention or review periods; do not retain identifiable information indefinitely "just in case".
- **Integrity and confidentiality:** use proportionate technical and organisational safeguards against unauthorised access, loss, alteration, disclosure or destruction.
- **Accountability:** record important decisions, responsibilities, controls, incidents, requests and reviews.

3. Accountability and roles

Max Pocock, as Lead Consultant and Data Protection Lead, is accountable for this policy, the company's processing decisions and escalation of material issues. This role title does not state or imply that Managed Services Ltd is legally required to appoint, or has appointed, a statutory Data Protection Officer.

Before giving a separately engaged human specialist, subcontractor or supplier access to personal information, Managed Services Ltd must:

1. confirm that access is necessary for a defined task;
2. complete proportionate due diligence on confidentiality, security and data location;
3. put written confidentiality and data-protection terms in place;
4. give role-specific instructions;
5. restrict access to the minimum required; and
6. remove access promptly when the work or need ends.

Everyone within scope must report a suspected incident, request, complaint or unauthorised instruction immediately to the Data Protection Lead.

4. Before processing starts

For each material processing activity or engagement, the company will record:

- the purpose and expected benefit;
- whether Managed Services Ltd is controller, joint controller or processor;
- categories of people and information involved;
- lawful basis and, where relevant, the condition for special-category or criminal-offence information;
- how the information is obtained, used, shared, stored, transferred and deleted;
- who needs access and why;

- privacy information to be given;
- retention or review dates;
- suppliers or subprocessors;
- security and incident routes; and
- whether a data protection impact assessment is required.

A data protection impact assessment will be completed before high-risk processing begins, including where new technology, vulnerable people, large-scale sensitive information, systematic monitoring or significant automated decisions create a likely high risk to people.

When processing children's information, the company will give particular weight to their interests, rights, development and ability to understand the processing. Services or research likely to be accessed by children must address the higher-protection requirements in force at the time.

5. Lawful, fair and transparent use

The company will choose the lawful basis that best fits the actual purpose; consent is not used by default. Where consent is relied on, it must be informed, specific, freely given, unambiguous, recorded and as easy to withdraw as to give.

Special-category and criminal-offence information will be processed only where both the ordinary lawful basis and the additional legal condition are recorded, with an appropriate policy document or other safeguards where required.

Privacy information will be concise, accessible and supplied at the appropriate time. It will identify the controller, purposes, lawful basis, recipients, transfers, retention approach, rights, complaint route and any significant automated decision-making relevant to the activity.

Personal information will not be reused for an incompatible purpose without a documented legal assessment and updated transparency where required.

6. Client data and processor duties

Where Managed Services Ltd processes personal information for a client, it will:

- act only on documented lawful instructions, unless law requires otherwise;
- ensure authorised people are bound by confidentiality;
- apply appropriate security;
- use a subprocessor only with the client's required prior authorisation and a compliant written contract;
- help the client with rights requests, security, breach response, impact assessments and regulatory enquiries as agreed;

- provide information reasonably required to demonstrate compliance and support agreed audits;
- tell the client promptly if an instruction appears to breach data-protection law; and
- return or securely delete personal information at the end of the service, subject to law and the contract.

Client ownership or instructions do not justify an unlawful act. A concern must be escalated before the affected processing continues, unless immediate action is required to protect a person or system.

7. Security and acceptable handling

The minimum handling rules are:

- use approved business accounts, devices, storage and transfer methods;
- enable multi-factor authentication where the service supports it;
- use strong unique credentials and never share them informally;
- apply least-privilege access and review access when roles or work change;
- keep devices, software and security protections supported and updated;
- encrypt data in transit and use device or storage encryption appropriate to the risk;
- verify recipients and attachments before sending sensitive information;
- keep identifiable material separate from analysis data where practical and use coded identifiers;
- maintain recoverable copies of critical information and test restoration proportionately;
- avoid local or removable-media copies unless necessary and protected;
- use secure deletion or verified return when information is no longer required; and
- protect paper records from unauthorised viewing, removal and disposal.

Identifiable personal information, confidential client information or safeguarding material must not be entered into public generative-AI services, consumer transcription tools or any unapproved system. Any technology-assisted processing must be assessed for purpose, lawful basis, data use, suppliers, security, transfers, retention, human oversight and contractual permission before use.

8. Retention and disposal

Every material information category must have a retention rule based on purpose, contract, legal need and risk. The company will:

1. set a deletion or review point when the information is collected;
2. reduce identifiability as soon as the purpose permits;

3. apply legal holds where deletion must be suspended;
4. document material deletion, return or approved archival transfer; and
5. review retained information after a purpose, contract or dispute ends.

Pseudonymised information remains personal information where re-identification is reasonably possible. Anonymisation must be effective before information is treated as outside data-protection law.

9. Individual rights and requests

The company will recognise and handle applicable rights, including access, rectification, erasure, restriction, objection, portability and safeguards relating to solely automated decisions.

Any channel can receive a rights request. The recipient must record and forward it immediately. Identity checks must be proportionate. Responses will be made without undue delay and generally within one month, subject to the legal rules on clarification, extensions, exemptions and third-party rights.

No one will be disadvantaged for exercising a data-protection right or raising a concern.

10. Data-protection complaints

People may make a data-protection complaint through the contact route shown in the relevant privacy notice, engagement document, website or company correspondence. No special wording or form is required.

Managed Services Ltd will:

- acknowledge a data-protection complaint as soon as practicable and no later than 30 days after receipt;
- make appropriate enquiries and keep the complainant informed without undue delay;
- separate any linked rights request and apply its legal timetable;
- communicate the outcome, reasons and any remedy without undue delay;
- record the complaint, evidence, decision and learning; and
- explain the person's right to complain to the Information Commissioner's Office.

The company aims to acknowledge ordinary complaints within two business days and provide a substantive outcome within 20 business days. Where complexity, dependency or fairness requires longer, it will explain the reason and next update date.

11. Personal-data breaches

Everyone within scope must report a suspected loss, misdirection, unauthorised access, disclosure, alteration, unavailability or destruction immediately. Lack of certainty is not a reason to delay internal reporting.

The Data Protection Lead will:

1. open an incident record and preserve relevant facts;
2. contain the incident and protect affected people;
3. assess what happened, the information and people affected, and the likely risk;
4. notify the client/controller promptly where Managed Services Ltd is a processor;
5. notify the Information Commissioner's Office without undue delay and, where feasible, within 72 hours of awareness when the legal threshold is met;
6. notify affected people without undue delay where the law requires it;
7. record the decision whether or not notification is required; and
8. implement corrective action and review effectiveness.

Safety, safeguarding, cyber-response and contractual notification duties run alongside this process.

12. Sharing and international transfers

Before disclosing personal information, the company will confirm the recipient, purpose, lawful authority, minimum fields, security method and any transparency requirement. Routine or repeated sharing will be governed by written terms.

Personal information will be transferred outside the United Kingdom only where the transfer is lawful and the required adequacy decision, recognised safeguard or exception is documented. Supplier location, remote access, support access and onward transfers must be considered, not only the address on the contract.

13. Monitoring, learning and review

The Data Protection Lead will review this policy at least annually and after a significant incident, regulatory change, new high-risk service, material supplier change or recurring complaint. Reviews will consider:

- processing and supplier records;
- rights and complaint timeliness;
- incident themes and corrective actions;
- access and retention reviews;
- training or briefing needs; and
- whether ICO fee registration, a statutory Data Protection Officer or additional specialist advice is required.

14. Official references

Official sources checked on 23 July 2026:

1. Information Commissioner's Office, Data protection principles, definitions and key terms - View official source
2. Information Commissioner's Office, Data protection by design and by default - View official source
3. Information Commissioner's Office, How to deal with data protection complaints - View official source
4. Information Commissioner's Office, Personal data breaches - a guide - View official source
5. Department for Science, Innovation and Technology, Data (Use and Access) Act 2025 - data protection and privacy changes - View official source

15. Document control

This controlled policy is reviewed at least annually. Tender-specific copies must be checked against the current company version and the buyer's requirements before issue.