Statom Group Access to Employee Email Accounts Policy HR-POL-075-01

1. Purpose
This policy sets out when and how Statom Group and all associated group companies may access an individual's work email account. We use this policy to protect business continuity, meet legal and regulatory duties, investigate misconduct, and safeguard Statom Group data, while respecting privacy and complying with UK GDPR and the Data Protection Act 2018.

2. Scope
This policy applies across Statom Group and all associated companies, subsidiaries, and trading entities ("Group Companies") and covers:

- All employees, workers, agency staff, consultants, directors, and contractors with a Group Company email account.
- All email systems provided or managed by Statom Group / Group Companies (including Microsoft 365/Google Workspace, shared mailboxes, archives, and backups).
- All devices and access methods used to access Group Company email.

3. Principles (Non-Negotiable)
Statom Group will only access mailboxes where access is:

- Lawful, necessary, and proportionate
- For a clear business purpose
- Authorised at the correct level
- Audited and time-limited
- Data-minimised (targeted retrieval first, full access only where justified)

4. Definitions

- Mailbox access: Any action that allows someone other than the account holder to view, search, export, forward, or otherwise process emails or mailbox contents.
- Targeted retrieval: IT extracts specific emails (by date range, client, subject keywords) rather than granting full access.
- Current worker: Still engaged by a Group Company in any capacity (employee/worker/contractor).
- Former worker: Engagement ended (leaver), including redundancy, resignation, dismissal, or end of contract.

5. Roles and Responsibilities

- Group IT / IT Provider: Implements access securely, applies time limits, ensures audit logs, and provides data securely.
- HR (Group or Company HR): Confirms status, ensures fairness, confirms process alignment with policies and employment law.
- Requester (Manager/Director): Provides written business rationale, confirms alternatives have been considered, limits request to what is needed.
- Authorising Director / Senior Manager: Approves access in line with Section 9.
- Data Protection Lead / DPO (if appointed): Advises on high-risk cases (e.g., sensitive data, disputes, investigations, large searches).

6. Acceptable Reasons for Access

Access may be approved for:

- Business continuity (absence, incapacity, urgent client/project commitments)
- Operational handover (role change, long-term leave)
- Legal/regulatory compliance (DSAR, litigation hold, regulator request)
- Investigation (misconduct, fraud, harassment, security incident, data leakage)
- Protection of Group assets (IP, confidential information, client obligations)

Access will not be approved for:

- Curiosity, informal monitoring, or personal disputes
- "Fishing expeditions"
- Convenience where alternatives exist (shared mailbox, delegation, targeted retrieval)

7. Current Workers: Access Rules

7.1 Default position

Statom Group does not provide managers with unrestricted access to a current worker's mailbox as standard.

7.2 Consent (preferred route where appropriate)

For operational cover (holiday, short absence, handover), we should seek the worker's written consent and use one of these options:

- Mailbox delegation to a nominated person (preferred)
- Shared mailbox / functional inbox arrangements
- Targeted retrieval of specific emails

Consent must be:

- Specific (who, what, why, how long)
- Recorded (email or signed form)
- Time-limited and reviewed

7.3 Access without consent (exceptional)

Access may be granted without consent only where:

- Consent cannot reasonably be obtained (e.g., incapacity) or
- Informing the worker would prejudice an investigation or
- There is a pressing legal/regulatory requirement

In these cases, Statom Group will:

- Record the lawful basis and justification (necessary and proportionate)
- Limit the scope (keywords/date ranges/folders wherever possible)
- Restrict access to named individuals only
- Set a strict time limit and remove access promptly
- Maintain audit logs
- Decide whether and when to inform the worker (case-by-case)

8. Former Workers: Access Rules

8.1 Ownership and records

Business emails and records created during engagement are Group Company records. After exit:

- The mailbox remains a Group record subject to retention/deletion rules.
- Access may be granted for legitimate business reasons, with controls.

8.2 Access options

For leavers, Group IT may:

- Provide targeted extracts (preferred), or
- Provide temporary audited access to an authorised person, or
- Convert mailbox to a shared mailbox for continuity where justified and time-limited

9. Approval Levels (Statom Group Standard)
All requests must be submitted via an IT ticket (or approved service desk process). No ticket = no access.
Current worker mailbox
- With consent for operational cover: HR + IT approval
- Without consent: HR + Company Director/Senior Manager + IT approval
- High-risk cases (sensitive data, disputes, investigations, broad searches): HR + Director + Data Protection Lead/DPO + IT

Former worker mailbox
- HR confirmation of leaver status + IT approval
- Escalate to Company Director/Senior Manager for sensitive, dispute-related, or legal hold matters

10. Controls and Safeguards
When access is approved, Statom Group will apply:
- Least privilege (minimum access needed)
- Time limits (start/end date, remove promptly)
- Audit logs (who accessed, when, actions taken)
- Confidentiality (use only for the approved purpose)
- Minimisation (targeted retrieval first)
- Secure handling (no personal email forwarding; store in approved systems only)

11. Employee Communications
Statom Group may inform workers when their mailbox is accessed unless:
- it would prejudice an investigation, or
- a legal/regulatory duty requires confidentiality

Where appropriate, we will provide a brief explanation of:
- purpose, scope, and duration of access (without disclosing confidential investigation details)

12. Monitoring and Privacy
Work email is provided for business use. Any personal use must comply with Statom Group Acceptable Use rules. Workers should not expect the same privacy as personal accounts. Statom Group will process personal data in line with its Privacy Notice, Data Protection Policy, and UK GDPR principles.

13. Leavers: Standard Mailbox Handling
On exit, Group IT will:
- Disable account access promptly (unless legal hold applies)
- Set an auto-reply and any approved forwarding arrangements
- Retain/archive mailbox in line with the Group retention schedule
- Delete when retention expires (unless preservation is required for legal reasons)

14. Non-Compliance
Unauthorised access to mailboxes is a serious breach of security and may result in disciplinary action (or contract action for contractors) and potential legal consequences.

15. Related Policies

- Statom Group Data Protection Policy
- Acceptable Use / IT & Communications Policy
- Information Security Policy
- Disciplinary Policy
- Records Retention Schedule
- Privacy Notice (Employee/Worker)

Appendix A: Minimum Ticket Requirements (mandatory)

Every request must include:

- Name of Group Company + requester name/role
- Mailbox owner name + email + current/leaver status
- Business purpose and justification
- Specific scope (date range, keywords, clients, folders)
- Who needs access (named individuals) and why
- Duration requested
- Alternatives considered (shared mailbox, delegation, targeted extract)
- HR approval confirmation
- Investigation/legal hold flag (yes/no)

SIGNED

Martina Oyite
Group HR Director

Review:	Annually	**Review**:	Annually
Date:	01/06/2025	**Date:**	01/06/2025
Next Review:	01/06/2025	**Next Review:**	01/06/2025