IGUAKO CAPITAL · Group policy

Information Barriers and Inside Information

This policy establishes the barriers that keep inside and confidential information received on one side of IGUAKO Capital from reaching persons on the other, and the procedures for bringing a person across a barrier when the work requires it. It divides the firm into a private side and a public side, requires an insider list for every transaction, governs wall-crossings, the restricted and watch lists and the cleansing of information, and sets the physical and electronic separations that give the barriers effect. It applies to all six divisions and to every member of staff.

CODE	CATEGORY	VERSION
IGC-MT-004	Markets and trading	3.1
EFFECTIVE	**REVIEW**	**OWNER**
2022-08-01	Annual; last reviewed August 2026, next review due August 2027	Head of the Control Room

1. Purpose and scope

The Investment Banking, Private Equity and Commercial Finance divisions receive information about companies that is not public, in the course of advising, investing and lending. The Quantitative Strategies and Private Wealth & UHNW divisions trade and advise in markets where that information would be valuable, and the Information & Data division publishes research. This policy exists so that the firm can do both sets of work without the first contaminating the second, and can show that it has.

The policy applies to every entity, office and desk and to every member of staff, contractor and adviser given access to the firm's systems. It applies to inside information and to confidential information about a client, a transaction or a counterparty, whether received from a client, a counterparty or a portfolio company or generated within the firm. It applies to information in any form, including conversation.

The Market Abuse Prevention policy governs the conduct the barriers prevent; the Personal Account Dealing policy governs the staff dealing the lists restrict; the Information Security policy governs the classification and handling of information, under which inside information is always Restricted. This policy governs the barriers themselves.

2. Definitions

The private side comprises the Investment Banking, Private Equity and Commercial Finance divisions, the deal-related legal and compliance staff, and any person wall-crossed on to a transaction. The public side comprises the Quantitative Strategies and Private Wealth & UHNW divisions, the Information & Data division's research and data teams, the trading desks and the sales and coverage staff who serve them.

Group functions, including finance, risk, technology and operations, are above the wall and are subject to the need-to-know rule for any specific transaction.

An insider list is the record, opened for each transaction or matter involving inside information, of every person who has access to that information, the date and time they received it, the reason and the date they ceased to have access. A wall-crossing is the controlled disclosure of inside information to a person on the public side, approved and recorded by the Control Room, which places that person on the insider list and under the private-side restrictions for the life of the matter.

The watch list is the confidential list of issuers about which the firm holds inside information; it is held by the Control Room and used for surveillance and clearance, and is not disclosed to the desks. The restricted list is the list of issuers in which trading, research and recommendations are restricted; it is disclosed to the desks and, by design, does not indicate why an issuer is on it. Cleansing is the confirmation that inside information has been made public or has ceased to be inside information, after which the persons on the insider list are released.

- Private side: Investment Banking, Private Equity, Commercial Finance, deal legal and compliance.
- Public side: Quantitative Strategies, Private Wealth & UHNW, research and data, trading desks, coverage.
- Above the wall: finance, risk, technology and operations, on a need-to-know basis per matter.

3. Principles

Information moves across the barrier only through the Control Room, only with a recorded reason, and only to a named person. It does not move because two colleagues share a floor, a client or a manager. A person who does not need inside information for their work does not receive it, whatever their seniority.

The firm restricts by issuer, not by suspicion. Once an issuer is on the watch list, the firm's ability to trade, research and recommend that issuer is limited according to the restricted list, and the limitation applies whether or not the persons on the public side know the reason for it.

The barrier is a system of records as well as a system of separation. The firm can show for any matter who knew what and when, and can show for any trade that the trader was not on an insider list for the issuer at the time the order was placed.

4. Requirements

A private-side team that receives inside information, or that expects to receive it within five business days, notifies the Control Room the same day. The Control Room opens an insider list, assigns the matter a code name, places the issuer on the watch list and, where the firm's involvement is likely to become public or the information affects a traded instrument, on the restricted list. Every person added to the insider list confirms in writing that they understand the restrictions before access is granted.

A wall-crossing is requested by the private-side team head, stating the person, the reason, the information to be disclosed and the expected duration, and is approved by the Head of the Control Room, or by the General Counsel where the Head of the Control Room is on the insider list. The person is briefed before the disclosure, added to the insider list, and restricted from trading, research and client advice in the issuer for the life of the matter. No more than two persons from any one public-side team are crossed on a single matter without the General Counsel's approval.

The private and public sides occupy separate access-controlled floors or zones in George Town, New York, London, Luxembourg and Singapore, and separate rooms in every other office. Electronic access to private-side documents is granted by insider list membership only, and every access to a matter's files is logged. Private-side and public-side staff do not share meeting rooms for a matter, do not use each other's printers and do not discuss any matter in a shared space.

Cleansing is confirmed by the Control Room when the information is made public or when the private-side team head confirms in writing that it has ceased to be inside information. The insider list is closed with the date, persons are released and the issuer is removed from the watch list. The restricted list is updated the same day. Where a matter is abandoned, the information is treated as inside information until the Control Room confirms that it has lost that character, which may be long after the matter ends.

- Same-day notification to the Control Room on receipt or expectation of inside information.
- Insider list, code name, watch list entry and written confirmation before access.
- Wall-crossing approved by the Head of the Control Room; no more than two per public-side team per matter.
- Separate access-controlled floors or zones in five offices and separate rooms elsewhere.
- Document access by insider list membership only, with every access logged.
- Cleansing confirmed by the Control Room before any person is released.

5. Roles and responsibilities

The Head of the Control Room owns this policy, maintains the insider lists, the watch list and the restricted list, approves wall-crossings and cleansings, and reports quarterly to the Compliance & Conduct Committee. The Control Room is a team of four within the compliance function, based in London and George Town, and its members are on every insider list by function and subject to the private-side restrictions permanently.

Private-side team heads are accountable for notifying the Control Room, for keeping their teams within the need-to-know rule and for confirming cleansing. Public-side desk heads are accountable for ensuring that no member of their desk trades, researches or advises in an issuer on the restricted list. The Head of Technology and Ethics is accountable for the electronic separations and the access logs.

Every member of staff who receives information they believe may be inside information, from any source and by any route, reports it to the Control Room the same day and does not act on it, disclose it or discuss it pending the Control Room's instruction. This includes information received socially or by mistake.

6. Monitoring and reporting

The Control Room reconciles the insider lists to the document access logs weekly and investigates every access by a person not on the list for that matter. The surveillance system checks every order against the watch list and every insider list in real time. Physical access logs for private-side zones are reviewed monthly. Insider lists open for more than 180 days are reviewed with the team head to confirm that the matter is live.

In the twelve months to 30 June 2026 the Control Room opened 58 insider lists, approved 41 wall-crossings and refused three, and confirmed 52 cleansings. The watch list held 31 issuers at 30 June 2026 and the restricted list 19. Access-log reconciliation identified two accesses by persons not on the relevant list, both by technology staff performing maintenance, both logged and reviewed, and neither involved the reading of matter content.

The Compliance & Conduct Committee receives the quarterly figures and every breach. Internal Audit reviews the lists, the reconciliations and a sample of wall-crossings annually, and an external review of the physical and electronic separations is performed every three years and reported to the Audit Committee.

7. Breaches

A breach is a failure to notify the Control Room, a disclosure across the barrier without a wall-crossing, an access to matter files by a person not on the insider list, a trade, research note or recommendation in an issuer on the restricted list, a discussion of a matter in a shared space, or a cleansing not confirmed before persons were released. Breaches are recorded on the day of discovery.

Any breach that may have resulted in inside information reaching a person who dealt is investigated under the Market Abuse Prevention policy and, where reasonable suspicion arises, reported to the relevant authority. The firm informs the client whose information was involved, where the client's interests may have been affected, within five business days.

Individual consequences follow the Code of Conduct; a deliberate disclosure across the barrier results in dismissal. Six breaches were recorded in the year to 30 June 2026: four late notifications to the Control Room, each within two business days, one research note on a restricted issuer withdrawn before distribution, and one shared-space discussion. None resulted in dealing.

8. Review

The Head of the Control Room reviews this policy annually and whenever an office opens, a division's activities change or a new information system is introduced. The review is approved by the Compliance & Conduct Committee, and any change to the definition of the sides is communicated to every member of staff before it takes effect.

The policy was first issued in August 2022 when the New York and Luxembourg offices reached the size at which physical separation became necessary. Version 3.1, approved in August 2026, added the 180-day open-list review and the two-person limit on wall-crossings. The next review is due in August 2027.

Key controls

- Control Room with sole authority over insider lists, the watch list, the restricted list, wall-crossings and cleansing.
- Insider list opened the same day, with a code name and written confirmation from every person added.
- Document access by insider list membership only, with weekly reconciliation of access logs.
- Real-time order screening against the watch list and every insider list.
- Separate access-controlled private-side zones in five offices with monthly physical access review.
- 180-day review of every open insider list.
- Annual Internal Audit review and three-yearly external review of the separations.

Related policies

- Market Abuse Prevention (IGC-MT-001)
- Personal Account Dealing (IGC-MT-003)
- Conflicts of Interest (IGC-CC-003)
- Information Security (IGC-DT-002)

Colophon

IGUAKO Capital is a work of institutional fiction by the Iguako Institute for Applied Unreality (iguako.tech). This document is part of that work. It creates no rights or obligations, describes no licensed entity and is not an offer, a contract, a client record or advice.