



ICIS Confidentiality Policy

Confidentiality Policy

Confidentiality Policy

1. Purpose

The purpose of this policy is to define how and when confidentiality is provided to a source and to outline how ICIS operates to ensure that data is only shared both internally and externally in an appropriate way. This policy seeks to balance the needs of sources to have confidentiality, to protect commercial and personal positions, and the desire of our readership for as clear, open, and transparent as possible news coverage of markets and prices.

Please note that the policy has a section that purely relates to the news and price reporting functions of ICIS.

2. Definitions

Information Staff: Employees whose management chain of command leads to the ICIS Editorial director and who are involved in the reporting of news and/or the price assessment process. This includes (but is not limited to): market analysts, news analysts, market reporters, news reporters, web editors, production staff and all managers of the above.

3. Market News and Price Reporting

ICIS reporters and the sources of information for their pricing reports have for many years interacted on the understanding that the identity of the sources would be confidential. These reports are an amalgam of information and not intended to document viewpoints from identifiable individuals. ICIS editorial staff should respect the reasonably held expectation of individuals and companies that they will not be identified except under the terms of any clear understanding that may have been reached between reporter and source, or where market norms involve the mention of company names.

Given that some markets have a relatively small number of participants of certain types or locations, it is not always possible to guarantee that the identity of a source could not be inferred. Reporters will do their best to avoid unintended identification, which can occur through the elimination in commentary of other market participants; through the use, especially in direct quotes, of a turn of phrase that may be particular to an

individual; or through excessive precision in identifying the number of sources used in a particular report or news story.

ICIS market commentaries are intended to be written with authority and some viewpoints are expressed without any attribution. In contrast, direct quotes and more specific (even if still generic) attributions in news stories are used to lend credibility and colour to the article.

Whether through published content or in discussion with market participants, ICIS reporters must not disclose their sources unless there is prior agreement with the source concerned.

Reporters must not agree to any conditions on the use of information that may create false or misleading views of the market among the readership, or that may impair the ability of ICIS to acquire the same information elsewhere and then publish it. In particular, ICIS reporters should be robust in using information in the public domain (such as corporate reports, regulatory filings, and information from public officials), and should refuse any requests to disguise or minimise the identification of that public information.

Given the wide range of interpretations of journalism phrases like "background only", "P&C", "off-the-record" and so on, the onus is on reporters to make sure the source understands how ICIS intends to use and attribute any such confidential information.

In rare cases it may be appropriate for the reporter to agree to allow a source to require pre-publication approval of how information is going to be presented. But these instances would be limited only to the information relevant to the source, and agreed to only with the consent of senior editorial management.

ICIS reporters must understand that the commitment to keep information confidential is undertaken by ICIS, not alone by an individual journalist. Upon request, the Managing Editors and Editorial director are entitled to know the identity of confidential sources and to review all notes and records of contact between a reporter and a confidential source.¹

Agreeing to confidentiality does not mean that ICIS will not require multiple sources to ensure a story is validated. In such a case, the reporter must be satisfied that the sources are genuinely independent of one another and are not connected behind the scenes.

¹ In the case of exceptionally sensitive reporting ICIS reporters may ask the Editorial director for permission to grant total confidentiality to a source. In such cases, intended to be extremely rare, the Editorial director may choose to ask for only a limited description of the source and the circumstances that support the request, and then may decide to waive the right to know the full identity of the source. Only the Editorial director may approve such a request.

4. All Employees and Agents of ICIS

Confidential information may not be disclosed by an employee or agent of ICIS to any person outside ICIS, including family members, for any reason other than an appropriate business purpose in light of the nature of the information. It is your responsibility to safeguard, secure and properly dispose of confidential information in accordance with the ICIS Record Retention Policy. This obligation extends to confidential information of third parties.

In many situations, confidential information must not be shared with other employees inside ICIS.

ICIS operates an information 'fire wall' between its Information Group, which produces market news and price assessments, and other commercial businesses such as its professional consulting and training groups, as well as its sales and marketing groups. ICIS staff who obtain confidential information through any of these functions should ensure that they do not share confidential information outside of their function. Where specific guidance or policy exists to govern the relationship between functions then employees must follow this to ensure confidentiality is maintained.

In the event of a breach of the 'fire wall', staff should consider themselves to be bound by the confidentiality obligations of the other function and should immediately report the breach to the Risk and Compliance Team.

5. Safeguarding Information

All employees and agents must take steps to protect the confidential nature of documents and information both on and off the company's premises. ICIS operates according to a corporate 'Computer Use Policy' which is a requirement for all employees and agents with IT systems access.

All employees and agents must only disclose confidential information on a "need-to-know" basis.

When it is necessary to transmit or transfer confidential information this must be done in accordance with the Computer Use Policy. This requires that employees must take due care to protect the security of the information, obtaining specialist advice where necessary. Confidential information in written form should not be left in public view or in an unsecured manner. Electronic information must not be left in public view nor must it be transmitted via an unsecured e-mail or electronic data transmission, and must never be posted on the Internet, including websites, electronic bulletin boards and social media.

Confidential or sensitive information also should not be discussed in public places such as in lifts (elevators), trains, on airplanes, at restaurants or other locations where it might be overheard. This includes discussing confidential information over the telephone in locations where it may be overheard.

NB. Employees are encouraged to take particular note of their use of mobile phones and laptops in public areas.

ICIS editorial staff generally do not record conversations with market contacts.² Rather, it is standard practice to make detailed notes of all reporting-related conversations or events. In order to ensure reporters follow methodologies and compliance policies ICIS will, from time to time, monitor reporter communications with market sources, including telephone, email and messaging service communications.

Where any editor, manager or other supervisory staff becomes aware of any confidential piece of information as a result of such monitoring they will become subject to the same confidentiality requirements and obligations as the reporter. Records will be kept of all such monitoring.

6. Legal Challenges to Confidentiality

If there is a situation where legal action is threatened to try to discover a source, it will be appropriate to consult with senior management, the Risk and Compliance Team and the legal team. In most cases, ICIS will use all reasonable efforts to maintain the confidentiality of the source.

7. Ownership of information and data

All information and data obtained, received or created by employees and agents of ICIS while working for ICIS is the property of ICIS and must therefore be treated accordingly and is subject to ICIS' various policies and processes. Information not generally available to the public as well as data obtained from any ICIS source should be considered confidential information unless there is prior agreement with the source of the information for the information to be released.

An employee's obligations with respect to confidential information of the Company continue even after their employment with the Company terminates.

² Please note that all calls to ICIS offices in China may be recorded. In such cases reporters will not have access to recordings without senior management approval.