

|                 |                                                                    |                 |                                    |                                                     |
|-----------------|--------------------------------------------------------------------|-----------------|------------------------------------|-----------------------------------------------------|
| User Group      | GCLIPS - Group Compliance Legal Integrity Property and Secretariat |                 |                                    |                                                     |
| Process:        | TSUK - Business Management System                                  | Document Title: | TSUK Confidential Reporting Policy |                                                     |
| Published date: | [Publishing Date]                                                  | Version:        | [Published Version]                | Document Owner: GCLIPS – Chief Legal Officer SC: No |

---

## Tata Steel UK Confidential Reporting Policy

### Introduction

Tata Steel UK (TSUK) is committed to conducting business with honesty and integrity, and all employees are expected to maintain high standards in accordance with the Tata Values and the Tata Code of Conduct. However, all organisations face the risk of things going wrong from time to time.

This policy is intended to make it clear that individuals can raise genuine concerns of wrongdoing without fear of victimisation, subsequent discrimination or disadvantage. This policy is intended to encourage and enable individuals to raise serious concerns within TSUK rather than overlooking a problem or 'blowing the whistle' outside.

The aims of this Policy are:

- (a) To encourage employees and also third parties (e.g. suppliers, contractors) to report suspected wrongdoing as soon as possible, in the knowledge that their concerns will be taken seriously and investigated as appropriate, and that their confidentiality will be respected;
- (b) To provide guidance as to how to raise those concerns;
- (c) To reassure employees and third parties that they are able to raise genuine concerns without fear of reprisals, even if they turn out to be mistaken; and
- (d) to provide reassurance that reports are considered in a professional manner and that a response is given to any concern raised.

### Scope

#### (a) Who is covered by the Policy?

This Policy applies to all employees, directors, consultants, contractors, trainees, temporary workers and agency workers of Tata Steel UK Limited and of all companies in its value chain. The term “employees” is used throughout this policy to cover all these categories of people who work for or provide services to TSUK.

Suppliers and other third parties are also encouraged to raise with TSUK any concerns they have about wrongdoing at TSUK. They are welcome to contact any senior manager to raise their concerns or they may use the confidential reporting system referred to below to raise a concern.

#### (b) Where does the Policy apply?

This Policy applies to TSUK and all its subsidiaries and entities within its value chain, wherever located. In addition, local procedures and/or rules may be in place that address how confidential reports (sometimes referred to as whistleblowing) are managed at a particular site or in a particular country, in accordance with local law. Details are available from local HR contacts or local compliance champions.

In some countries, legislation offers additional protection to individuals who make disclosures about certain types of activities (such as corruption). TSUK is committed to complying with all relevant laws relating to whistleblowing and protected disclosures, in addition to this Policy.

### (c) What type of concerns are covered by the Policy?

This Policy applies to concerns about activities which suggest one or more of the following types of wrongdoing:

- failure to comply with any of TSUK's policies, rules or guidelines (e.g. damage or misuse of company property or assets, breach of IT policies);
- criminal activity (e.g. fraud, false accounting, theft);
- bribery;
- failure to comply with any legal obligation or regulatory requirements (e.g. contractor falsely invoicing TSUK; false reporting of financial or other information);
- danger to health and safety;
- danger to TSUK's IT-systems, networks or other communication means (e.g. phone system, VoIP, web-pages, SharePoint etc.);
- danger to the environment;
- failure to comply with the Tata Code of Conduct (e.g. unethical behaviour);
- breach of data privacy rules or legislation;
- failure to comply with quality standards;
- unauthorised disclosure of confidential information;
- other conduct likely to damage the reputation of TSUK;
- the deliberate concealment of any of the above.

The processes referred to in this Policy are not for use as a means to challenge commercial decisions, nor as a mechanism for obtaining confidential business information. Any matters raised for such purposes will be rejected as not applicable to this Policy and the confidential reporting systems.

Employees are encouraged to report personal grievances (relating to e.g. selection procedures, job evaluation, personal performance reviews) through the appropriate channels and procedures in HR, as they can be better addressed in that way. Any such matters reported through the confidential reporting channel may be referred to HR to deal with in accordance with HR procedures, where more appropriate.

**Concerns about an immediate threat of physical harm or damage to property or persons should not be reported through the Confidential Reporting System. Local Security or emergency services, as appropriate, should be contacted in such circumstances.**

### Responsibility for this Policy

TSUK's Legal Compliance team has overall responsibility for this Policy, and for reviewing the effectiveness of actions taken in response to concerns raised under this Policy. All cases which are reported through the Confidential Reporting System will be reported on a quarterly basis to the TSUK Compliance and Integrity Committee and on a 6 monthly basis to the TSE Audit Committee (with any individuals' names removed in order to maintain confidentiality).

The Legal Compliance Team has responsibility for the day-to-day operation of this Policy. All employees are responsible for the success of this Policy and should ensure that they use it to disclose any suspected danger or wrongdoing.

## Raising a Concern

Where possible, TSUK employees should raise any concerns of wrongdoing with their line manager or another TSUK manager, in person or in writing. Third parties should raise any concerns with their respective line manager or with a TSUK manager, in person or writing. The manager may be able to agree a way of resolving the concern quickly and effectively. In some cases the relevant manager may refer the matter to the Chief Legal Officer & Company Secretary, or any another member of the Legal Compliance team who may then arrange for an investigation of the complaint as detailed below. Material breaches of TSUK's Policies should be referred to the sponsor of the relevant policy as indicated in the policy document.

However, where an employee feels unable to or uncomfortable with speaking to their line (or other) manager, or having done so feels that the concern has not been addressed, employees are encouraged to report their concern:

- (a) using the Company's Confidential Reporting System; or
- (b) to Chief Legal Officer & Company Secretary, or another member of the Legal Compliance team; or
- (c) to the Chair of the TSE Audit Committee.

Contact details are annexed to this Policy and set out in the TSUK intranet and on the supplier portal [www.tatasteel.europesuppliers.com](http://www.tatasteel.europesuppliers.com)

## Confidential Reporting System

TSUK subscribes to an external, independent service that runs a confidential reporting system for TSUK. Employees or third parties may make reports using the Freephone telephone service or via web access at any time. Employees are requested to provide sufficient details to enable the report to be fully investigated. Any supporting evidence that can be provided will be welcomed. Reports can be provided in the employee's preferred language.

TSUK employees do not have access to the telephone number or email address from which the report was made – only to the detail provided in the report itself. TSUK will only make contact with the employee reporting the concern through the feedback process in the Confidential Reporting System (using the reference number given), unless the employee agrees to another means of communication.

## Assessment and Investigations

After an initial assessment of any report made through the Confidential Reporting System, a decision will be made as to whether an investigation is required and, if so, who is best placed to carry out such an investigation of the alleged wrongdoing. Investigations strictly follow Group Policies, operational guidelines and procedural rules as well as legal rules in the respective country. They will be carried out sensitively and in a confidential manner.

Reports to the Confidential Reporting System, whether anonymous or not, will be shared only with those who have a "need to know", so that a suitable course of action can be determined, an effective investigation conducted (where applicable) and for appropriate corporate reporting purposes. Those with a need to know may in some instances include third parties such as TSUK's external auditors, external legal counsel, or law enforcement bodies, to the extent necessary.

Employees making a confidential report will be kept informed of the progress of any investigation through the Confidential Reporting System. However, the need for confidentiality may prevent the provision of specific details of any investigation. Details of disciplinary or legal actions taken against individuals will not be provided, unless required by law. Confidential business information and personal data will not be provided.

All concerns will be dealt with fairly and in an appropriate way, protecting the rights of any accused persons as well as the employee making the report. TSUK will comply with all applicable data protection laws in managing reports made to it.

### Confidentiality and Anonymity

If a concern is raised confidentially, every effort will be made to keep confidential the identity of the employee raising the concern, unless required by law to disclose the identity. In some circumstances it may be necessary for the person investigating the allegation to know the reporting employee's identity. Every effort will be made to discuss this first with the employee concerned.

Employees may make reports anonymously (where permitted by the law of the relevant country) but this does make it much more difficult (and in some cases impossible) to investigate the allegation properly. An investigation process itself may reveal the source of the information to the investigator. In such circumstances, this information will not be shared and every effort will be made to maintain the anonymity of the reporting employee. If an employee has any concerns about possible reprisals if their identity were to be revealed (or deduced) they are encouraged to raise those concerns with HR, the Chief Legal Officer & Company Secretary, or another member of the Legal Compliance team.

### Safeguards

TSUK recognises that the decision to report a concern can be a difficult one to make. Employees who raise genuine concerns under this Policy will be supported, even if they turn out to be mistaken.

However, misuse of the system to intentionally make false, bogus or malicious complaints will be subject to disciplinary or other action.

TSUK will not tolerate any harassment or victimisation of employees who report concerns and will take appropriate action to protect individuals who raise a concern in good faith from any adverse repercussions. Any employee who believes that he or she has suffered any such treatment, should inform HR, the Chief Legal Officer & Company Secretary or another member of the Legal Compliance team. Anyone who threatens to retaliate or retaliates against employees who report concerns in any way will be subject to disciplinary or other action.

**January 2025**

## CONTACTS

|                                                      |                                                                                                                                                                                                                          |
|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Confidential Reporting System: Integrity Line</b> | <a href="https://tsuk.integrityline.com">https://tsuk.integrityline.com</a><br><br>The country-specific telephone numbers to contact Integrity Line are to be found on the TSUK intranet. <a href="#">Integrity Line</a> |
| <b>Chief Legal Officer and Company Secretary</b>     | Mr Alastair Page<br><br>18 Grosvenor Place, London, SW1X 7HS<br><br><a href="mailto:alastair.page@tatasteeleurope.com">alastair.page@tatasteeleurope.com</a>                                                             |
| <b>Head of Ethics &amp; Compliance Management</b>    | Mrs Clare Cook<br><br>Abbey General Offices, Port Talbot, SA13 2NG<br><br><a href="mailto:clare.cook@tatasteeleurope.com">clare.cook@tatasteeleurope.com</a>                                                             |
| <b>Chair, Audit Committee, Tata Steel Europe</b>     | Mr Deepak Kapoor<br><br>C/O<br><br><a href="mailto:secretariat@tatasteeleurope.com">secretariat@tatasteeleurope.com</a>                                                                                                  |

## Change Register

| Revision Date | Version | Description of Revision | Responsible person |
|---------------|---------|-------------------------|--------------------|
| March 2025    |         | Transferred to TSUK DMS |                    |
|               |         |                         |                    |
|               |         |                         |                    |