

Group Whistleblowing Policy



THE ENGINEERED STONE GROUP

Group Whistleblowing Policy

Owner	Claire Vasco	An environmental logo featuring a green tree on the left, a white winding path leading towards the tree, and the text 'THINK Before you print' in green and 'SAVE a tree' in white on a green background.
Position	Personal Assistant	
Effective Date	1 st March 2024	
Name	Group Whistleblowing Policy	

Contents

Introduction	3
Aim of this policy.....	3
Scope of this policy.....	3
What is Whistleblowing?.....	4
When to blow the whistle?.....	4
How to blow the whistle?.....	5
The Investigation Process	5
<i>The whistleblowing team</i>	5
Receiving a message.....	5
Investigation.....	6
Whistleblower protection	6
Processing of personal data.....	7
Deletion of Data	7
Legal basis of the Whistleblowing guidance	7
Personal data processor.....	7
Appendix A	8

Group Whistleblowing Policy

Introduction

The Engineered Stone Group (ES Group) are committed to conducting their business fairly, honestly and with transparency and in compliance with all legal and regulatory obligations. We expect that all Engineered Stone Group directors, employees and anyone acting on our behalf to do the same and to maintain the highest standards of ethical behaviour. However, all organisations face the risk of things going wrong from time to time. A culture of openness and accountability is essential in order to prevent such situations occurring and to address them when they do occur.

A key aspect of ensuring and maintaining The ES Group's commitment to conducting business with such integrity and in an open and fair manner is providing a robust whistleblowing policy and reporting channel for the group so that all colleagues feel able to report any wrongdoing in confidence. At The ES Group, we encourage employees to report any concerns as soon as these arise; such concerns can be of any nature, including any matters in connection with The ES Group's personnel, as well as customers, suppliers and other third parties.

Aim of this policy

The aim of this policy is therefore to:

- Encourage and empower colleagues to speak up and 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.
- Provide colleagues with guidance as to how to raise those concerns.
- Reassure colleagues that they will be able to raise genuine concerns without fear of reprisals, even if they turn out to be mistaken.
- Encourage a culture of openness.
- Ensure compliance with the relevant legislation.

This is not a policy to be used in order to question The ES Group's financial decisions or business strategy, nor should it be used to raise matters which would normally be considered under an HR grievance procedure or are already the subject of a disciplinary procedure. The below sets out in more detail what type of behaviour this policy covers and what should be reported pursuant to this policy.

Scope of this policy

This policy applies to all ES Group's entities and personnel (including directors, executives, employees, contractors, agency workers, casual workers, consultants and trainees) no matter which team they work in or which office. It relates to actions by such personnel as well as any concerns a colleague may have with one of The ES Group's customers, suppliers or any other third parties which The ES Group interacts with or does business with.

Group Whistleblowing Policy

What is Whistleblowing?

Whistleblowing is the term used when an employee passes on information concerning wrongdoing. This can be called “making a disclosure” or “blowing the whistle”. The wrongdoing will typically (although not necessarily) be something they have witnessed at work.

To be covered by Whistleblowing law, the employee who is making a disclosure must reasonably believe two things: The first is that they are acting in the public interest, and the second is that the employee must reasonably believe that the disclosure tends to show past, present or likely future wrongdoing.

When to blow the whistle?

As noted above, The ES Group wants to hear about such conduct that is unlawful, dishonest, or unethical as soon as possible and is committed to addressing it.

The below provides examples of the types of misconduct or behaviour that could give rise to a report. However, it is not an exhaustive list and The ES Group encourages all colleagues to report any behaviour or incidents which they have concerns about.

- Criminal activity or offences, including fraud, theft and embezzlement.
- Corruption, bribery or blackmail.
- Financial malpractice, impropriety or mismanagement.
- Facilitating tax evasion.
- Failure to comply with any legal or professional obligations or regulatory requirements.
- Conduct likely to damage The ES Group's reputation or financial wellbeing.
- Actions which endanger the health and safety of The ES Group's personnel or the public.
- Actions which cause damage to the environment.
- The deliberate provision of false information to public officials.
- A miscarriage of Justice.
- Unauthorised disclosure of confidential information.
- The deliberate concealment of information relating to any of the above matters.
- Bullying, harassment or discrimination
- Any retaliation against someone for speaking up or “whistleblowing”.

Everyone has a responsibility to report any such misconduct or potential misconduct as soon as they become aware of it. If you are uncertain whether something is within scope of this policy, it is preferable that any concerns are reported rather than kept to oneself.

A person who blows the whistle does not need to have firm evidence for expressing suspicion. However, deliberate reporting of false or malicious information is prohibited. Such abuse of the whistleblowing service can be treated as a serious disciplinary offence.

Group Whistleblowing Policy

How to blow the whistle?

All of the options below include escalation to members of staff who are fully trained in whistleblowing reporting and procedures. Irrespective of the opinion exercised therefore, the whistleblowing procedures of the ES Group has in place ensure that you will be taken through and will fully understand the overall process and next steps.

There are two ways to raise a concern:

- ✓ Alternative 1: Contact a supervisor or manager within the organisation.
- ✓ Alternative 2: Anonymous or confidential messaging through the whistleblower communication channel to the whistleblowing team: <https://report.whistleb.com/engstone>

We encourage anybody who shares their suspicions to be open and honest with their identity. All messages received will be handled confidentially. For those wishing to remain anonymous, we offer a channel for anonymous reporting. The whistleblowing channel enabling anonymous messages is administered by WhistleB, an external service provider. All messages are encrypted. To ensure the anonymity of the person sending the message, WhistleB deleted all meta data, including IP addresses. The person sending the message also remains anonymous in the subsequent dialogue with the responsible receivers of the report.

The Investigation Process

The whistleblowing team

Access to messages received through our whistleblowing channel is restricted to appointed individuals with the authority to handle whistleblowing cases ("Whistleblowing-Team"). The team is made up of the following:

- Jens Heymann: Group Chief Financial Officer
- Luis Aguado: HR Director Spain
- Monika Królikowska: HR Director Poland & UK
- Claire Vasco: Personal Assistant to the Executive Team

Their actions are logged and handling is confidential. When needed, individuals who can add expertise may be included in the investigation process. These people can access relevant data and are also bound to confidentiality.

If a person raises a concern directly to a supervisor, manager or by contacting the whistleblowing team in person, such messages are also treated according to these guidelines.

Receiving a message

Upon receiving a message, the whistleblowing team decides whether to accept or decline the message. If the message is accepted, appropriate measures for investigation will be taken.

Group Whistleblowing Policy

The whistleblower will receive an acknowledgement within 48 hours of receipt of the concern.

The whistleblowing team may not investigate the reported concern if:

- The alleged conduct is not reportable conduct under these Whistleblowing guidelines
- The message has not been made in good faith or is malicious
- There is insufficient information to allow for further investigation
- The subject of the message has already been solved

If a message includes issues not covered by the scope of these Whistleblowing guidelines, the whistleblowing team should take appropriate action to get the issue solved.

The whistleblowing team will send appropriate feedback within 2 (maximum 3 months for complex cases) months upon the date of receiving the report.

Sensitive or personal information about anybody mentioned in the message should not be included if it is not necessary for describing the concern.

Investigation

All messages are treated seriously and in accordance with these Whistleblowing guidelines.

- No one from the whistleblowing team, or anyone taking part in the investigation process, will attempt to identify the whistleblower.
- The whistleblowing team can, when needed, submit follow-up questions via the channel for anonymous communication.
- A message will not be investigated by anyone who may be involved with or connected to the misgiving.
- The whistleblowing team decides if and how a whistleblowing message should be escalated.
- Whistleblowing messages are handled confidentially by the parties involved.

Appendix A details the Case Management Workflow and summarises the process.

Whistleblower protection

A person expressing genuine suspicion or misgiving according to these guidelines will not be at risk of losing their job or suffering any form of sanctions or personal disadvantage as a result. It does not matter if the whistleblower is mistaken, provided that he or she is acting in good faith.

Subject to considerations of the privacy of those against whom allegations have been made, any other issues of confidentiality, a whistleblower will be kept informed of the outcomes of the investigation into the allegations.

In cases of alleged criminal offences, the non-anonymous whistleblower will be informed that his/her identity may need to be disclosed during judicial proceedings.

Group Whistleblowing Policy

Processing of personal data

The whistleblowing service may collect personal data on the person specified in a message, the person submitting the message (if not sent anonymously) and any third person involved, in order to investigate facts of the declared misdeeds and inappropriate behaviour. This processing is based on statutory obligations and the legitimate interest of the controller to prevent reputational risks and to promote an ethical business activity. The provided description and facts under this processing are only reserved to the competent and authorised persons who handles this information confidentially. You may exercise your rights of access, of rectification and opposition, as well as limited processing of your personal data in accordance with the local data protection legislation. These rights are subject to any overriding safeguarding measures required to prevent the destruction of evidence or other obstructions to the processing and investigation of the case. Data is stored in the EU.

Deletion of Data

Personal data included in whistleblowing messages and investigation documentation is deleted when the investigation is completed, with the exception of when personal data must be maintained according to other applicable laws. Permanent deletion is carried out 30 days after completion of the investigation. Investigation documentation and whistleblower messages that are archived should be anonymised under GDPR; they should not include personal data through which persons can be directly or indirectly identified.

Legal basis of the Whistleblowing guidance

This policy is based on the EU General Data Protection Regulation, EU Directive on whistleblower protection and national legislation on whistleblowing.

Personal data processor

WhistleB Whistleblowing Centre Ab (World Trade Centre, Klarabergsviadukten 70, SE-107 24 Stockholm) responsible for the whistleblowing application, including processing of encrypted data, such as whistleblowing messages. Neither WhistleB nor any sub-suppliers can decrypt and read messages. As such, neither WhistleB nor its sub-processors have access to readable content.

Group Whistleblowing Policy

Appendix A

Case Management Workflow



THE ENGINEERED STONE GROUP

