

FRAUD POLICY

Fletcher Building expects the highest standards of honesty and integrity from all employees and contractors and will not tolerate fraudulent behaviour.

Fraud doesn't only have a financial cost, it can also damage our reputation and that has an impact on us all.

We expect employees to take reasonable steps to safeguard our funds and assets against fraud, loss and unauthorised or inappropriate use. We are committed to taking prompt action to fully investigate and address any suspected fraud cases.

The purpose of this policy is to establish guidelines and procedures to prevent, detect and respond to fraudulent activities within the FB Group.

NEED TO KNOW

- We will **not tolerate** fraud of any kind.
- Managers must ensure appropriate control processes are designed, implemented, maintained and monitored. Managers must also ensure that teams **are aware of, and meet**, their obligations within these control processes.
- Employees have a responsibility to be alert to the signs of fraud and **report** suspected cases of fraud without delay.
- Business units must report any suspected fraud immediately to the GM Group Assurance and the Group CFO via a dedicated mail address – Fraud.Reporting@fbu.com. All frauds are reported to the Audit and Risk Committee twice a year.
- All cases of suspected fraud will be independently **investigated** with appropriate action taken.
- We will consider all measures to **recover losses** (including investigation costs).
- Employees who commit fraud face the prospect of **disciplinary action and/or referral to relevant external authorities**. We will hand the matter to the authorities for appropriate actions to be pursued once we are satisfied we should do so.

This policy applies to: all Fletcher Building directors, officers, employees, former employees, independent contractors and subcontractors, consultants, temporary agency personnel and secondees of Fletcher Building Limited and its subsidiaries.

It is expected non-wholly owned subsidiaries and applicable joint venture/alliances will adapt these rules and guidelines to be consistent with this policy.

EXPLANATORY AND GUIDANCE NOTES

1. Definition

The word “fraud” covers a wide range of behaviours and activities. It generally refers to an intentional and dishonest act that involves deception or misrepresentation and where the perpetrator obtains (or potentially obtains) an advantage for themselves or another person. It can be committed by an individual or individuals against the FB Group, our customers, or other external parties.

Fraud includes, but is not limited to, the examples below:

Asset misappropriation	Fraudulent statements and behaviours
<ul style="list-style-type: none">• Theft of cash• False payment requests• Cheque fraud• Billing schemes• Misuse of accounts• Theft of inventory or fixed assets• Theft of information or IP (including, for example, identity theft)• False invoicing (including, for example, vendor collusion)• Payroll fraud• Accounts receivable fraud• Deliberate misuse of resources	<ul style="list-style-type: none">• Knowingly approving false or deliberately misleading purchase orders or invoices for payment• Knowingly providing false, incomplete or misleading information• Deliberate mishandling of or misreporting money or financial transactions• Presenting false credentials or qualifications• Document forgery with a view to personal gain or gain for another person• Intentional improper revenue recognition• Intentional misstatement of assets, liabilities and/or expenses• Knowingly submitting a false timesheet, leave form or expense claim/declaration or knowingly failing to submit a leave form

2. Preventing fraud

Code of Conduct

All managers and team leaders are expected to maintain a culture of honesty and openness in their workplace and ensure consistent and correct application of control processes in their area of responsibility.

Managers and team leaders should also:

- Ensure Fletcher Building’s Employee Code of Conduct and this policy are made available to all employees and they have an understanding of their obligations
- Ensure employees are not discouraged from questioning events or processes or reporting suspected fraud
- Regularly promote reporting channels including FBUCall to employees and others subject to this policy.

Control Environment and Review Processes

FB Group's businesses must take all appropriate measures to establish a rigorous control environment to deter fraud. These measures should include (but not limited to):

- A system of business appropriate Delegated Financial Authorities (DFA's) that are consistent with the Group DFA's
- The segregation of employee responsibilities and oversight in critical business processes
- Appropriate system access given to employees following the principle of least privilege (i.e. access is granted that is appropriate for an employee's current duties. Access is not granted for duties that are not part of an employee's responsibility)
- Regular reconciliation processes
- Anti-fraud training and awareness programs for employees.

The control environment will be reviewed on a regular basis via:

- Business units completing a quarterly control self-assessment review.
- Regular internal audits.

3. Reporting fraud

It is the duty of every individual to uphold the FB Group's values and report any suspicious activities in accordance with this policy.

If you uncover or suspect a fraud or theft you should report your findings or suspicions immediately to your manager or supervisor. If you don't feel comfortable doing this, or wish to remain anonymous you can also raise any concerns directly with:

- Your site or business unit's or division's People and Performance Manager
- Directly with the Fletcher Building General Manager of Group Assurance by email (Fraud.Reporting@fbu.com)
- Through our confidential, externally-managed hotline FBuCall

A person who reports actual or suspected fraud may remain anonymous, and can be protected under the relevant local legislation.

When reporting suspected fraud you should retain any documentary evidence upon which your concerns were based, and provide these in reporting to the relevant appropriate personnel. You should not discuss any suspicions with the alleged fraudster(s), work colleagues or other employees except those above.

Business units must report any suspected fraud immediately to the GM Group Assurance and the Group CFO. The following email address should be used for this reporting – Fraud.Reporting@fbu.com.

4. Our response to fraud

Investigation process

Upon receipt of a suspected fraud the GM Group Assurance will make an evaluation of the severity and nature of the issue to determine whether an internal (either BU lead or Internal Audit led) or external investigation is required and will ensure that the appropriate resources are secured for the investigation.

In all circumstances the person selected to conduct the investigation will be independent and objective and will not be in a position of direct authority over any of the people involved in the complaint.

Any investigation must:

- ensure that any suspected fraud has been investigated impartially, thoroughly and as far as reasonably possible; and
- ensure any conclusions are justified based on evidence obtained.

Acting on proven fraud cases

The factors and behaviours relevant to the company’s decision to take internal disciplinary action, or to prosecute will vary from case to case.

Business units should always consult with the FB legal team before deciding on referring matters to the authorities. When it is considered appropriate, the company will pass on its investigation file to the relevant authorities to allow them to pursue any action that the authorities consider appropriate. The company must not agree to any settlement on the basis that it will not inform the authorities.

When sufficient evidence is available the company must take steps to protect its asset position by taking steps to recover any losses and/or obtaining a freezing order.

Questions on this policy? Discuss with your direct manager, your People and Performance Manager, or the General Manager of Group Assurance by email (Fraud.Reporting@fbu.com).

Printing this policy: All our official policies are updated electronically and available on [Matrix](#) so before relying on a printed copy please check you have the latest version.

Other relevant policies: [Whistleblowing \(Wrongdoing\) Disclosure Policy](#), [Anti-bribery and Corruption](#), [Trade Practices Policy](#), [Artificial Intelligence Policy](#), [Code of Conduct](#).

Updates to this policy document			
Version	Action	Authority	Date
1			April 2019
2	Inclusion of action to refer frauds to authorities. Confirmation of internal email address for reporting Fraud.		August 2020
3	Review	Policy contact	December 2023
Next review due: December 2025			