ETHICS HOTLINE POLICY

OBJECTIVE

The management of James Hardie Industries plc, including its subsidiaries and affiliates (collectively, the **Company**), expects all of its employees to observe high ethical standards in the performance of their duties, to observe all laws and regulations governing business transactions and to use corporate funds and assets only for appropriate business purposes. The Company believes that unethical or illegal conduct should not go unreported. The purpose of this Ethics Hotline Policy (this **Policy**) and the establishment of the Ethics Hotline, together with the Company's Global Code of Business Conduct, are to promote ethical and legal behavior and to encourage you to, and outline a means by which you can, report improper conduct so that it can be dealt with appropriately.

The objective of the Ethics Hotline is to provide a confidential means for employees and other eligible individuals to report suspected unethical or improper conduct, or any other concerns, in a manner that is outside the normal chain of command. The Ethics Hotline is designed to help ensure compliance with all applicable laws and regulations, promote the sound business practices embodied in Company policies and help avoid misconduct.

This Policy will be reviewed on an annual basis by the Audit Committee of the Company's Board of Directors. The Appendices may be updated, if necessary, more frequently.

Depending on where you are employed, we have set out additional information on the specifics of the Ethics Hotline and on special reporting requirements in your location in the Appendices below. Where applicable, the Appendices detail alternative reporting channels that may be available in your location.

If you are based in the EU, please also refer to the Company's Privacy Notice in Appendix XII for further information about the way the Company processes the personal data of EU employees in connection with the Ethics Hotline and beyond.

REPORTING

Whenever you have a concern about a party's ethical or business conduct, you should first attempt to address the issue with your supervisor, a representative in the Human Resources Department, an attorney or other representative within the Legal and Compliance Department, or directly with the Company's Chief Legal Counsel.

However, if you have a concern regarding the reporting of an issue or believe the issue may not be or has not been properly addressed, you are also encouraged to report the issue through the

Ethics Hotline (to the extent allowed by applicable law) in accordance with the procedures set out in this Policy.

Nothing in this Policy is intended to prevent any individual from reporting information to federal, state, provincial, or local law enforcement, regulatory, or administrative agencies when an individual has reasonable cause to believe that a violation of law has occurred. A report to law enforcement, regulatory, or administrative agencies may be made instead of, or in addition to, a report directly through the Ethics Hotline or any other reporting method specified in this Policy/its Appendices.

ACTIVITIES AND ISSUES TO BE REPORTED

Examples of activities or events that may constitute a breach of Company policy or an unauthorized act that the Company would expect employees and other eligible individuals to report include, but are not necessarily limited to, the following:

- accounting or audit irregularities;
- antitrust or competition or trade practice violations (e.g., unauthorized discounts, cartel conduct such as price fixing, market sharing etc.);
- breach of the Global Code of Business Conduct;
- breach of any applicable law or regulation;
- bribes or kickbacks;
- corporate espionage or sabotage;
- conflicts of interest;
- unauthorized disclosure of proprietary information and/or personal data;
- employment issues (e.g., discrimination/unlawful harassment, drug abuse, etc.);
- environmental, health and safety issues;
- falsification of Company records;
- fraud or theft of cash or Company property;
- insider trading; and
- other misconduct, dishonest or illegal activity.

Again, the above list is not exhaustive. Any concerns regarding unethical or improper conduct should be promptly reported using the guidelines described in this Policy.

Please also refer to the additional information contained in the Appendices that further detail the issues which can be reported through the Ethics Hotline in your location.

ANONYMITY AND CONFIDENTIALITY

Subject to applicable laws, individuals who report suspected business misconduct through the Ethics Hotline do not have to give their name and may choose to remain anonymous.

Subject to applicable laws, information provided by an individual when reporting suspected misconduct or during the course of an investigation will, to the extent practical, be treated as confidential except as may be reasonably necessary under the circumstances to facilitate an investigation, take remedial action, or comply with applicable law. All information submitted via the Ethics Hotline, or otherwise, will be processed and stored in an appropriate manner to protect its confidentiality and in accordance with applicable data protection laws.

Nothing in this Policy prohibits or is intended to restrict or impede employees from discussing the terms and conditions of their employment with co-workers or disclosing information as permitted by applicable laws.

Certain additional statutory protections that may apply to officers and employees located in Australia, New Zealand, the Philippines, Germany, the United Kingdom, Spain, the Netherlands, Italy, France, Denmark, and Ireland are explained in **Appendices I-XI**. Appendices I-XI will be reviewed on an annual basis by the Chief Legal Counsel and/or somebody under his/her direction.

INCIDENT REPORTS AND DISSEMINATION

Any report made through the Ethics Hotline will be recorded by the third-party provider in an incident report.

The third-party provider will make incident reports available as soon as reasonably possible to the Ethics Hotline Principals or the Head of Legal Europe, depending on which country the report originated from, and will immediately escalate an incident report to the Company's designated emergency contacts in the event that the third-party provider deems that the report meets the following criteria:

- it constitutes a threat or harm to employees, customers or operations; or
- it is a significant incident that is expected to recur within 24 hours of the time that it is first reported.

Incident reports received for non-EU countries will be provided to and reviewed by one or more of the **Ethics Hotline Principals**, which generally includes the Company's Chief Legal Counsel, Assistant General Counsel – Employment, Chief Human Resources Officer, and Vice President – Internal Audit, or other delegated representatives, depending on the nature of the report.

For incident reports received by the Ethics Hotline from EU countries, the incident report will be provided to the Head of Legal Europe (or external legal counsel if the Head of Legal Europe is identified as a party in the incident report), who will remove any personally identifiable information (PII) and send the anonymized report to the Ethics Hotline Principals.

To the extent one of the Ethics Hotline Principals is named in a report, that Ethics Hotline Principal will not receive or review the incident report. The Chairman of the Audit Committee will receive

a copy of reports that expressly reference the CEO, CFO, Chief Legal Counsel, and Chief Human Resources Officer.

All reports will be investigated in accordance with applicable laws and Company policies. Following the investigation, the Company will take any appropriate corrective action(s) in accordance with applicable laws.

INVESTIGATION PROCEDURES

One or more of the Ethics Hotline Principals will review the incident reports and will: (i) assign the investigation of the reported incident to appropriate personnel (the **Investigator**), and (ii) oversee the investigation of the reported incident.

For incident reports originating from the EU countries, the Ethics Hotline Principals will review anonymized incident reports and (i) assign the investigation of the reported incident to appropriate personnel in the EU (the **Investigator**), and (ii) oversee the investigation of the reported incident on an anonymized basis.

RESOLUTION

All reports to the Ethics Hotline will be addressed as quickly as possible. If the individual submitting the report identifies himself/herself, the Investigator will coordinate follow-up contact with such individual as soon as reasonably practicable depending on the circumstances. The purpose of the initial contact shall be to inform the individual that the report is being investigated. After a report has been addressed, the Company will advise the reporting party that the concern has been addressed and, if appropriate, of the resolution, to the extent possible and in accordance with applicable laws and Company polices.

All information obtained during the investigation shall be treated as confidentially as possible under the circumstances, to the extent permitted by applicable law and in accordance with all applicable data protection laws and regulations.

NO RETALIATION

All forms of unlawful retaliation are prohibited. The Company strictly prohibits any form of retaliation against an individual for reporting suspected violations of law, violations of Company policy, unethical conduct, or other improper conduct in good faith, regardless of whether the claim is substantiated or not, or otherwise participating in an investigation of or legal proceeding regarding any suspected violation of law, violation of Company policy, unethical business conduct, or other improper business conduct.

If you believe that you have been or are being subjected to any unlawful retaliation, please immediately report such matter to: (i) a representative in your local Human Resources

Department; (ii) a representative in your local Legal Department; (iii) the Chief Legal Counsel; or (iv) the Ethics Hotline.

Subject to applicable laws, employees who intentionally, maliciously or for their own personal benefit make false allegations may be subject to disciplinary action, up to and including termination of employment. Furthermore, if the Company determines that an employee participated in, or had knowledge of, misconduct but did not report it and should have, such employee may be subject to disciplinary action up to and including termination of employment.

CONTACTING THE ETHICS HOTLINE

The Company has contracted with Navex Global Inc. (**Navex**) to receive reports submitted via the Ethics Hotline. Many corporations utilize Navex as an external provider to oversee and administer their ethics hotlines.

You may submit a report of suspected misconduct to the Ethics Hotline via the internet or by phone. To submit a report via the internet, please go to www.jameshardie.ethicspoint.com and follow the instructions provided. To submit a report by phone, please dial the following number for your applicable location from an outside line:

Call Origination Location	Call Type	Phone Number
US	Toll Free	1-800-620-6935
Australia	Toll Free	Dial International Toll-Free Service Number (**ITFSN**): 1800-339276
Austria	Toll Free	Dial ITFSN: 0800-291870; or Dial 0-800-200-288 and at the English prompt dial 800-4720519
Belgium	Toll Free	Dial 0-800-100-10 and at the English prompt dial 800-4720519
Canada	Toll Free	1-800-472-0519 (English) or 1-855-350-9393 (French)
Czech Republic	Toll Free	Dial ITFSN: 800-142-637
Denmark	Toll Free	Dial 800-100-10 and at the English prompt dial 800-4720519
France	Toll Free	Dial ITFSN: 0800-91-5881
Germany	Toll Free	Dial 0-800-225-5288 and at the English prompt dial 800472-0519
Ireland	Toll Free	Dial 1-800-550-000 and at the English prompt dial 800472-0519
Italy	Toll Free	Dial ITFSN: 800-790332
Luxembourg	Toll-Free	Dial Global Inbound Services (**GIS**) Number: 80085226
Netherlands	Toll Free	Dial GIS: 08004030003
New Zealand	Toll Free	Dial GIS: 0508023451
Philippines	Toll Free	Dial ITFSN: 1-800-1-114-0165; or Dial 105-11 or 10105511-00 and at the English prompt dial 800-472-0519.
Poland	Toll Free	Dial ITFSN: 00-800-151-0255

Spain	Toll Free	Dial ITFSN: 900-991498; or Dial 900-99-0011 and at the English prompt dial 800-472-0519
Sweden	Toll Free	Dial GIS Number: 0201408260
Switzerland	Toll Free	Dial 0-800-890011 and at the English prompt dial 800-4720519
United Arab Emirates	Toll Free	Dial 8000-021, 8000-555-66 (du) or 8000-061 (military, USO or cellular) and at the English prompt dial 800-4720519
United Kingdom	Toll Free	Dial ITFSN: 0808-234-6675
Other (except in the countries noted above)	Collect Call	Tell your local international telephone operator that you would like to place a reverse charge call to the United States and give them the following number: 770-582-5240

NOTE: Landline and mobile phone connectivity can vary by location and telephone carrier. In the event that you experience a connection issue with the number listed for your location, please utilize the website portal listed above to lodge your report or contact the Ethics Hotline via the toll-free number listed for the United States or the collect call dialing option listed at the bottom of the table.

ADMINISTRATION OF THE ETHICS HOTLINE

- The Company's relationship with the external third-party provider is managed and overseen by the Company's Chief Legal Counsel.

- The Ethics Hotline is answered by interview specialists employed by the third-party provider and is operational 24-hours a day, 365 days a year. Submissions made via the internet can also be made at any time.

- All reports submitted in EU countries will be received in the EU and all data relating to those reports will be hosted in the EU.

- The third-party provider employs multi-lingual interview specialists and can make such specialists available upon request.

- Except as set forth herein, all calls/submissions are confidential, and individuals do not have to give their names.

- You may choose not to provide your name if you choose to remain anonymous. Depending on your location, you may even be strongly encouraged not to provide your name.

- An interview specialist will ask for details about your concerns and will document what you tell him or her in an incident report.

- Because the Company is a multinational corporation with multiple locations, you are encouraged to provide as many details as you can. This will help to ensure that the incident is properly investigated and resolved.

- Individuals submitting anonymous reports will be asked to follow-up with the third-party provider through the Ethics Hotline at an appropriate time following their initial submission. At that time, individuals may be asked additional questions or be asked for additional information.

- All individuals submitting reports will be given a report number to reference in subsequent interactions with the third-party provider.

RECORDS RETENTION

Documentation of concerns reported via the Ethics Hotline, subsequent investigations, and dispositions will be retained in accordance with the Company's record retention policy, the guidelines established by the Legal and Compliance Department, and all applicable data protection laws and regulations.

PERIODIC SUMMARY REPORTING TO AUDIT COMMITTEE

At the end of every quarter, the Ethics Hotline Principals, at the direction of the Chief Legal Counsel, will prepare a summary of incidents reported via the Ethics Hotline during the foregoing quarter and furnish it to the Audit Committee for the quarterly Audit Committee meeting.

APPENDIX I

AUSTRALIAN WHISTLEBLOWER PROCEDURES

James Hardie Australia Pty Limited (**JHA**) has adopted these Australian Whistleblower Procedures (**Procedures)** with effect on and from 1 January 2020 to give effect to its obligations under section 1317AI (2) of *Corporations Act 2001* (Cth) (**Corporations Act**). Part A of these Procedures detail available "whistleblower" protections under the *Corporations Act* (Australia **General Whistleblower Regime**) and Part B of these Procedures provides some additional information about available protections under the *Taxation Administration Act 1953* (Cth) (**Taxation Act**) (Australia **Tax Whistleblower Regime**).

These Procedures apply to officers, employees and other eligible whistleblowers of JHA and of the other Australian incorporated companies forming part of the James Hardie group from time to time. JHA and those other companies are referred to in this Appendix I to the Policy collectively as **the Australian Subsidiary Companies** and each individually as an **Australian Subsidiary Company**.

These Procedures contain a general description of the operation of the relevant provisions of the Corporations Act and the Taxation Act. The available protections vary according to the circumstances and subject matter of the contemplated disclosure. If you are in any doubt about how any aspect of these Procedures or the available protections may apply to you, you should seek your own legal advice.

You should read this Appendix I in conjunction with the Policy that applies to all James Hardie group entities, including the Australian Subsidiary Companies. These Procedures supplement the Policy insofar as it applies to the Companies.

The purpose of this Appendix I and Policy is to assist in identifying wrongdoing that may not be uncovered unless there is a safe and secure means for disclosure. This Appendix I and Policy encourages officers, employees and related persons who are aware of possible wrongdoing to disclose wrongdoing in the spirit of the James Hardie group's values, and to deter wrongdoing in line with the Global Code of Business Conduct.

PART A – AUSTRALIA GENERAL WHISTLEBLOWER REGIME

To be protected under the Australia General Whistleblower Regime, an individual must first fall within a certain class of persons as outlined below (**Eligible Whistleblower**). Eligible Whistleblowers are **not** required to identify themselves when making a disclosure and will be eligible for protection in respect of eligible disclosures even if they make the disclosure anonymously.

Who is an Eligible Whistleblower?

You will be an Eligible Whistleblower if you are or were:

- an officer or employee of an Australian Subsidiary Company (e.g. current and former employees who are permanent, part-time, fixed-term or temporary, interns, secondees, managers, and directors);
- an individual who supplies services or goods on a paid or unpaid basis to an Australian Subsidiary Company;
- an employee of a person supplying services or goods on a paid or unpaid basis to an Australian Subsidiary Company (e.g. current and former contractors, consultants, service providers and business partners);
- an associate (as defined in the Corporations Act) of an Australian Subsidiary Company;
- a spouse, child or dependent of any of the former; or
- a dependent of a spouse of any of the former.

What are Eligible Disclosures?

To be eligible for protection under the Australia General Whistleblower Regime, the Eligible Whistleblower must be disclosing information that they have reasonable grounds to suspect concerns misconduct, or an improper state of affairs or circumstances, in relation to one or more of the Australian Subsidiary Companies or any of their related bodies corporate (**Eligible Disclosures**). This may not necessarily include a contravention of a particular law. However, Eligible Disclosures include information concerning the commission of an offence under, or other contravention of, the Corporations Act or certain other specified Commonwealth laws. They also include information concerning conduct that constitutes an offence against any other law of the Commonwealth that is punishable by imprisonment of 12 months or more. Information that indicates a significant risk of danger to public safety or the stability of or confidence in the financial system, even if the conduct does not involve a breach of a particular law, are also disclosable matters.

Examples of disclosable matters under Eligible Disclosures include, but are not limited to:

- fraud, money laundering or misappropriation of funds;
- offering or accepting a bribe;
- financial irregularities; and
- failure to comply with, or breach of, legal or regulatory requirements;
- and engaging in, or threatening to engage in, conduct against a person who has made a disclosure or is believed or suspected to have made, or be planning to make, a disclosure.

An Eligible Whistleblower who makes an Eligible Disclosure can still quality for protection under the Australia General Whistleblower Regime even if their disclosure turns out to be incorrect.

What about personal work-related grievances?

Personal work-related grievances are generally **not** protected under the Australia General Whistleblower Regime. Such grievances include matters which relate to an individual's current or former employment and which do not concern disclosable matters protected by the Australia General Whistleblower Regime, which do not concern an allegation of detriment caused to the individual related to disclosures protected by the General Whistleblower Regime, or which do not have significant implications for an Australian Subsidiary Company or for James Hardie Industries plc.

Examples of personal work-related grievances include interpersonal conflicts between employees and decisions relating to the engagement, transfer, promotion, suspension, demotion, termination or discipline of employees. Per the JHA Workplace Complaint Policy personal work-related grievances and other issues and concerns that are not covered by this Policy can be communicated to your supervisor/manager, your People and Performance Business Partner or a member of the James Hardie Legal and Compliance Department.

A personal work-related grievance may still qualify for protection if it is a mixed report that includes or is accompanied by information about misconduct, discloses breach of employment or other laws punishable by imprisonment for a period of 12 months or more, discloses conduct that represents a danger to the public, suggests misconduct beyond the discloser's personal circumstances, if the discloser suffers from or is threatened with detriment for making a disclosure or if they are seeking legal advice or legal representation about the operation of the Australia General Whistleblower Regime.

Which disclosures are Protected Disclosures?

An Eligible Disclosure made by an Eligible Whistleblower may attract certain protections under the Australia General Whistleblower Regime as described further below.

The Australia General Whistleblower Regime protects four categories of Eligible Disclosure:

- Initial Disclosures;
- Public Interest Disclosures;
- Emergency Disclosures; and
- Legal Advice Disclosures,

all as further defined below (together, **Protected Disclosures**).

1. Initial Disclosures

If you are an Eligible Whistleblower and you make an Eligible Disclosure to one or more of the following persons or regulatory bodies, then your disclosure (**Initial Disclosure**) should attract certain statutory protections under the Australia General Whistleblower Regime. Those persons or bodies are:

- an officer or senior manager of an Australian Subsidiary Company or of a related body corporate;
- an internal or external auditor or member of an internal or external audit team conducting an audit on an Australian Subsidiary Company or a related body corporate;
- an actuary of an Australian Subsidiary Company or of a related body corporate;
- a person or body prescribed by regulation; or
- a person authorized by an Australian Subsidiary Company to receive such disclosures;

(together, the **Eligible Recipients**), OR

- a Commonwealth authority designated for this purpose, which includes the Australian Securities & Investments Commission (**ASIC**) and the Australian Prudential Regulation Authority (**APRA**) (each a **Designated Regulatory Authority**).

You may wish to seek additional information before formally making a disclosure. To obtain additional information, you may contact the Chief Legal Counsel (JHIplcComplianceOfficer@jameshardie.com), the Assistant General Counsel – APAC, the Associate General Counsel - Employment or an independent legal adviser.

2. Public Interest Disclosures

If you have made an Initial Disclosure to a Designated Regulatory Authority and, after 90 days, you do not have reasonable grounds to believe that action has been or will be taken to address the matters to which the disclosure related, and you have reasonable grounds to believe that doing so would be in the public interest, you may make a protected second disclosure (**Public Interest Disclosure**).

You will need to firstly provide a written notice to the Designated Regulatory Authority that received the Initial Disclosure identifying your Initial Disclosure and indicating your intention to make a Public Interest Disclosure.

A Public Interest Disclosure will only be protected under the Australia General Whistleblower Regime if it is made to a Member of Parliament or to a journalist, where a journalist is an individual who works in a professional capacity for any of the following:

- a newspaper or magazine;
- a radio or television broadcasting service; or
- an electronic service, including a service provided through the internet, which operates on a commercial basis or is operated by a body providing a national

broadcasting service, and is similar to a newspaper, magazine or radio or television broadcast.

The Public Interest Disclosure must contain no more detail than is necessary to inform the recipient of the misconduct or improper state of affairs or circumstances that are the subject of the disclosure. You are encouraged to contact the Chief Legal Counsel (JHIplcComplianceOfficer@jameshardie.com) or an independent legal adviser before making a Public Interest Disclosure to ensure that your disclosure is eligible for protection under the Australia General Whistleblower Regime.

3. Emergency Disclosures

If you have made an Initial Disclosure to a Designated Regulatory Authority and you have reasonable grounds to believe that your information relates to substantial and imminent danger to the health or safety of humans or the natural environment, you may make a second protected disclosure (**Emergency Disclosure**).

You will need to firstly provide a written notice to the Designated Regulatory Authority that received the Initial Disclosure identifying your Initial Disclosure and indicating your intention to make an Emergency Disclosure.

An Emergency Disclosure will only be protected if it is made to a Member of Parliament or a journalist (as defined above), and the Emergency Disclosure must contain no more detail than is necessary to inform the recipient of the substantial and imminent danger. You are encouraged to contact the Chief Legal Counsel (JHIplcComplianceOfficer@jameshardie.com) or an independent legal adviser before making an Emergency Disclosure to ensure that your disclosure is eligible for protection under the Australia General Whistleblower Regime.

4. Legal Advice Disclosures

Information you disclose to a legal practitioner is protected if you have disclosed it to obtain legal advice or representation in relation to the operation of the Australia General Whistleblower Regime. If the legal practitioner concludes that your disclosure does not relate to disclosable matters, your disclosure to the legal practitioner will still remain protected under the Australia General Whistleblower Regime.

What protections apply?

The key protections available to Eligible Whistleblowers under the Australia General Whistleblower Regime include:

1. Confidentiality and Anonymity

If you make a Protected Disclosure, your identity, as well as any information that is likely to identify you, must be kept confidential by the recipient. There are a limited number of circumstances where your identity and/or any related information will not remain confidential, namely where the information is disclosed:

- by the recipient to ASIC or APRA;
- by the recipient to a member of the Australian Federal Police (**AFP**);
- by the recipient to a legal practitioner in order to obtain legal advice or representation in relation to the Australia General Whistleblower Regime;
- with your consent; or
- where the recipient is ASIC, APRA or a member of the AFP, if they disclose to a Commonwealth, State or Territory authority to assist the authority in the performance of its duties.

Information that is likely to identify you may also be disclosed where the disclosure is reasonably necessary to investigate the misconduct or improper state of affairs to which your disclosure relates, and the disclosing recipient takes all reasonable steps to reduce the risk of you being identified.

Outside of the exceptions listed above, it is illegal for a person to identify a discloser or disclose information that is likely to lead to their identification. If you believe you have experienced a breach of confidentiality, you may lodge a complaint through the Ethics Hotline, with the Chief Legal Counsel (JHIplcComplianceOfficer@jameshardie.com) or with a regulatory authority such as ASIC, APRA or the ATO (where appropriate), for investigation.

If you make a Protected Disclosure you are not required to disclose your identity or information that is likely to identify you to a court or tribunal unless it is necessary for the operation of the Australia General Whistleblower Regime, or if the court or tribunal finds that it is necessary for the administration of justice.

You may choose to remain anonymous while making a disclosure, over the course of the investigation and after the investigation is finalized. However, we strongly encourage that you identify yourself so that we can properly investigate the matter. We are committed to protecting and supporting you if you make a Protected Disclosure and will ensure that we do so. You may remain anonymous by contacting an Australian Subsidiary Company through the Ethics Hotline or by email anonymously or using a pseudonym. For the avoidance of any doubt, if your disclosure is sent from an email address from which your identity cannot be determined and you do not identify yourself in the email, such an email will be treated as anonymous. You may refuse to answer questions that you think could reveal your identity, include during follow-up conversations. If you choose to remain anonymous, you will need to maintain an ongoing two-way channel of communication so that follow-up questions and feedback may be conveyed.

In practice, the confidentiality of your identity will be protected through the following measures:

- all personal information or references to the discloser witnessing an event will be redacted and the discloser will be referred to in a gender-neutral context;
- disclosures will be handled and investigated by qualified staff who have undergone appropriate training;
- all paper and electronic documents and other materials, including call records relating to disclosures, will be stored securely;
- access to all information relating to a disclosure will be limited to those directly involved in managing and investigating the disclosure;
- subject to the discloser's consent, only a restricted number of people who are directly involved in handling and investigating a disclosure will be made aware of a discloser's identity or information that is likely to lead to the identification of the discloser;
- communications and documents relating to the investigation of a disclosure will not to be sent to an email address that can be accessed by staff not involved in the investigation; and
- each person who is involved in handling and investigating a disclosure will be reminded about the confidentiality requirements, including that an unauthorised disclosure of a discloser's identity may be a criminal offence.

2. Protection from legal proceedings

If you make a Protected Disclosure, you will generally be protected from civil, criminal and administrative liability as a result of having made the disclosure, including disciplinary, contractual or other action such as termination of your employment contract where your disclosure would otherwise have constituted a breach of that contract, or resulted in prosecution for unlawfully releasing information, or disciplinary action for making the disclosure.

Where you have made an Initial Disclosure to a Designated Regulatory Authority, or a Public Interest Disclosure or Emergency Disclosure, the information that is the subject of your disclosure cannot generally be used as evidence against you in criminal proceedings or proceedings imposing a penalty, unless the reliability of your information is the subject of the proceedings. However, this does not prevent you being subject to civil, criminal or administrative liability or action in respect of your own conduct revealed by the disclosure.

3. *Protection from detrimental acts or omissions*

The Australian Subsidiary Companies are committed to protecting Eligible Whistleblowers who have made Protected Disclosures from retaliatory action. Retaliatory action includes dismissal, injury, demotion or other detrimental alteration of position or duties, discrimination, harassment or intimidation, damage to property, reputation, business or financial position or any other damage, or threats of any of the foregoing, whether to you as the Eligible Whistleblower or to any other third party (together, **detriment** or **detrimental conduct**). A threat of detriment may be express or implied, or conditional or unconditional, and you do not have to actually fear that the threat will be carried out in order for the conduct to be considered as a "threat".

For the avoidance of doubt, actions which may not be considered as detrimental conduct include administrative action that is reasonable for the purpose of protecting a discloser from detriment (such as transferring the Eligible Whistleblower to a different office to protect them from detriment), and managing the Eligible Whistleblower's performance in accordance with a Company's performance management framework and policy where the Eligible Whistleblower has exhibited unsatisfactory work performance. In the event that administrative or management action is taken, the relevant Australian Subsidiary Company will take measures to ensure that its reasons are understood ahead of implementing the action.

In practice, you will be protected from detriment or detrimental conduct through the following measures:

- processes for assessing the risk of detriment against a discloser and other persons (for example, other staff who might be suspected to have made a disclosure) will commence as soon as possible after receiving a disclosure;
- work-arounds to minimize the risk of detriment, for example temporary or permanent office location transfers, re-assignment to another role at the same level, or other modifications to the workplace or way you perform your work duties, or such re-assignment and re-location of other staff involved in the disclosable matter, may be available as appropriate;
- management will be trained to ensure they are aware of their responsibilities to maintain the confidentiality of a disclosure, to address the risks of isolation or harassment, manage conflict, and ensure fairness when managing the performance of, or taking other management action relating to, a discloser;
- support services including counselling, legal or other professional services to assist with stress, time or performance management, or managing other challenges resulting from the disclosure or its investigation, are available; and

if you experience detriment in relation to making a Protected Disclosure,

- there is a complaint mechanism in place to enable you to lodge a complaint, whereby investigation of your complaint will be conducted as a separate matter and reported to the Chief Legal Counsel or another Ethics Hotline Principal;

- appropriate measures will be taken to reduce the impact of detriment, such as disciplinary action taken against those perpetrating the detrimental conduct, or in relation to you as the discloser, allowing extended leave, developing a career development plan including new training and career opportunities, or other compensation packaging options; and
- in any case, you may seek independent legal advice or contact regulatory bodies including ASIC, APRA or the ATO (where appropriate).

If you or any third party is exposed to any kind of detriment (including loss, damage or injury) as a consequence of making a Protected Disclosure, and we have not taken reasonable precautions and exercised due diligence to prevent the detrimental conduct, you have a right to bring civil or criminal proceedings, or proceedings for civil penalties, against the person or persons causing the detriment (**Detrimental Party**). We encourage you to seek independent legal advice should such a situation arise. The court may:

- grant an injunction to prevent, stop or remedy the effects of the detrimental conduct;
- order the Detrimental Party to compensate you or any affected third party for loss, damage or injury suffered as a result of the detrimental conduct;
- order the Detrimental Party to apologise to you or any affected third party;
- where you have been terminated from your position, order the reinstatement of your position or one at a comparable level; or
- order that additional damages be paid to you or any affected third party.

If you choose to seek compensation for breach of the protections available under the Australia General Whistleblower Regime in a court, you will generally not have to pay costs unless you have instituted the proceedings unreasonably.

How do I make a protected disclosure?

If you are aware of or reasonably suspect misconduct or an improper state of affairs or circumstances relating to an Australian Subsidiary Company or any of its related bodies corporate, you are encouraged to first attempt to address the issue by disclosing the information to your supervisor/manager, your People and Performance Business Partner, a member of the Legal and Compliance Department or to the Chief Legal Counsel. You may also make a disclosure through the confidential Ethics Hotline.

All of these persons are authorised by each Australian Subsidiary Company to receive such disclosures for the purposes of the Australia General Whistleblower Regime and your disclosure will be treated accordingly.

If you choose to make a Protected Disclosure to a person who is an Eligible Recipient but who is **not** one of the nominated persons above, your disclosure may still attract relevant protections under the Australia General Whistleblower Regime. However, you are encouraged to bring the matter to the attention of one or more of the persons nominated above so that the Company is in

a position to investigate the matter and take appropriate action in accordance with these Procedures and this Policy.

How will my protected disclosure be investigated?

Any Protected Disclosure will be investigated in conformity with the Policy. The key steps that will be taken following receipt of a disclosure are outlined below. The duration of each step is dependent on the nature and complexity of the disclosure:

1. ***Initial assessment***: Depending on the nature of the claim, the disclosure will be assessed by the Eligible Recipient together with any or all of the Ethics Hotline Principals to determine if the disclosure qualifies for protection as a Protected Disclosure, and whether a formal, in-depth investigation is required.
2. ***Assessment scoping***: Depending on the nature of the claim, the Ethics Hotline Principals will then determine the nature and scope of the investigation, the person(s) within or external to the Australian Subsidiary Companies who will lead the investigation and any external support required.
3. ***Investigation***: You will be notified upon the commencement of the investigation. Please note that the investigation process may be limited to the extent that you are not able to be contacted (for example, where you have made your disclosure on an anonymous basis and have not provided a means of contact).
4. ***Documentation and reporting***: The findings from the investigation will be compiled in a report that will be documented and reported to the Ethics Hotline Principals. Confidentiality of the discloser's identity will be maintained in the report. The report will be stored securely and can only be accessed by those persons on the investigation team and the Ethics Hotline Principals. The discloser will be notified about the findings of the investigation to the extent appropriate. There may be some circumstances where it may not be appropriate to provide full details of the outcome to the discloser.
5. ***Review***: If, as the discloser, you are not satisfied with the outcome of the investigation, you may contact the Ethics Hotline or another Eligible Recipient for a review. The review will be led and conducted by persons not involved in the handling and investigating of the Protected Disclosure, and they will provide their review findings to the Chief Legal Counsel. The Australian Subsidiary Companies are not obliged to reopen an investigation and can conclude a review if it is found that the initial investigation was conducted properly, or new information is not available or would not change the findings of the investigation. You may lodge a complaint with a regulator, such as ASIC, APRA or the ATO (where appropriate) if you are not satisfied with the outcome of the investigation.

Fair treatment of parties involved in disclosures

You, as well as any other employees or related parties who are mentioned in the Protected Disclosure, will be treated fairly and you will be protected from detriment under the Australia General Whistleblower Regime as adopted by these Procedures. You will not, however, be entitled

to immunity from prosecution or other disciplinary action for any misconduct in which you were involved simply because you reported it.

PART B – AUSTRALIA TAXATION WHISTLEBLOWER REGIME

The Taxation Act may provide additional protections where the subject matter of the disclosure relates to the tax affairs of an Australian Subsidiary Company or its associates and the discloser considers that the information may assist the recipient to perform functions or duties in relation to the tax affairs of the Australian Subsidiary Company or an associate. The term "tax affairs" in this context means affairs relating to taxes imposed, assessed or collected by the Federal Commissioner of Taxation.

The categories of Eligible Whistleblower under the Australia Taxation Whistleblower Regime are similar to those under the Australia General Whistleblower Regime. Eligible Recipients under the Taxation Whistleblower Regime include the Commissioner of Taxation, an auditor or member of the audit team, a registered tax agent or BAS agent providing services to an Australian Subsidiary Company, an employee or officer of an Australian Subsidiary Company who has functions or duties relating to its tax affairs or another person authorized to receive such disclosures. In addition to the persons authorized by each Australian Subsidiary Company to receive disclosures under the Australia General Whistleblower Regime, the Global Tax Director is a person authorized to receive disclosures relating to tax affairs.

The types of Protected Disclosure under the Australia Taxation Whistleblower Regime are generally similar to those under the Australia General Whistleblower Regime, and includes disclosure relating to misconduct or an improper state of affairs in relation to the tax affairs of an Australian Subsidiary Company or an associate where the whistleblower considers the information may assist the recipient to perform functions or duties in relation to those tax affairs. There is no equivalent to a Public Interest Disclosure or Emergency Disclosure under the Australia Taxation Whistleblower Regime.

Rights to protection of an Eligible Whistleblower's identity and protection from legal proceedings, victimization and detrimental conduct are broadly similar to those under the Australia General Whistleblower Regime.

A person contemplating making a disclosure relating to the tax affairs of any of an Australian Subsidiary Companies or their associates should inform themselves about the specific eligibility requirements, and the potential protections available to them, under the Australia Taxation Whistleblower Regime in the specific circumstances of the contemplated disclosure. If you are in any doubt about how any aspect of this Policy, these Procedures or the available protections may apply to you, you should seek your own legal advice.

Further information available about this Policy and these Procedures

This Policy and these Procedures are publicly available on the James Hardie Industries plc Investor Relations website, and all officers and employees can access the Policy through the Hardie People Policies SharePoint page. Please contact your People and Performance Business Partner, a member of the Legal and Compliance Department or the Chief Legal Counsel, if you

have any questions about these Procedures or the Policy. Regular training sessions will be conducted to ensure officers and employees have an up-to-date understanding of this Policy, Appendix I, and these Procedures. Specialist training will be provided to staff members who have specific responsibilities under this this Policy, Appendix I, and these Procedures, including Eligible Recipients in non-Australian James Hardie entities, which will be communicated to the staff members appropriately.

APPENDIX II

NEW ZEALAND WHISTLEBLOWER PROCEDURES

James Hardie NZ Holdings Limited (**JHNZ**) has adopted these New Zealand Whistleblower Procedures (**Procedures)** with effect on and from February 2023 to give effect to its obligations under the *Protected Disclosures (Protection of Whistleblowers) Act 2000* (the **Protected Disclosures Act**). These Procedures set out and detail the available "whistleblower" protections under the Protected Disclosures Act (**New Zealand General Whistleblower Regime)**.

These Procedures apply to officers, employees and other eligible whistleblowers of the New Zealand incorporated companies forming part of the James Hardie group from time to time. JHNZ and those other companies are referred to in these Procedures collectively as **the NZ Subsidiary Companies** and each individually as an **NZ Subsidiary Company**.

These Procedures contain a general description of the operation of the relevant provisions of the Protected Disclosures Act. The available protections vary according to the circumstances and subject matter of the contemplated disclosure. If you are in any doubt about how any aspect of these Procedures or the available protections may apply to you, you should seek your own legal advice.

You should read these Procedures in conjunction with the Policy that applies to all James Hardie group entities, including the NZ Subsidiary Companies. These Procedures supplement the Policy insofar as it applies to the NZ Subsidiary Companies.

NEW ZEALAND GENERAL WHISTLEBLOWER REGIME

To be protected under the New Zealand General Whistleblower Regime, an individual must first fall within a certain class of persons as outlined below (**Eligible Whistleblower**). Eligible Whistleblowers are **not** required to identify themselves when making a disclosure and will be eligible for protection in respect of eligible disclosures even if they make the disclosure anonymously.

Who is an Eligible Whistleblower?

You will be an Eligible Whistleblower if you are:

- an employee of a NZ Subsidiary Company;
- a former employee of a NZ Subsidiary Company;
- a person seconded to a NZ Subsidiary Company;
- an individual who is engaged or contracted under a contract for services to do work for a NZ Subsidiary Company;

- a person concerned in the management of a NZ Subsidiary Company (including a person who is a member of the board or governing body of a NZ Subsidiary Company); or
- a person who works for a NZ Subsidiary Company as a volunteer without reward or expectation for that work.

What are Eligible Disclosures?

To be eligible for protection under the New Zealand General Whistleblower Regime, the Eligible Whistleblower must:

- be disclosing information about a serious wrongdoing in relation to one or more of the NZ Subsidiary Companies, or any of their related bodies corporate; and
- believe on reasonable grounds that the information is true or is likely to be true (even if this belief is mistaken); and
- wish to disclose the information so that the serious wrongdoing can be investigated;
- substantially comply with the requirements of the Protected Disclosures Act, even if you do not technically comply; and
- wish the disclosure to be protected under the provisions of these Procedures, even if you do not expressly refer to the Protected Disclosures Act (together, **Eligible Disclosures**).

Your disclosure will not be protected by the Protected Disclosures Act if you act in bad faith or the information you are disclosing is protected by legal professional privilege.

What about personal work-related grievances?

Except in the limited circumstances defined below, personal work-related grievances are **not** protected under the New Zealand General Whistleblower Regime. Such grievances include matters which relate to an individual's current or former employment and which do not concern an allegation of detriment caused to the individual related to disclosures protected by the New Zealand General Whistleblower Regime, or which do not have significant implications for a NZ Subsidiary Company or for James Hardie Industries plc.

Examples of personal work-related grievances include interpersonal conflicts between employees and decisions relating to the engagement, transfer, promotion, suspension, demotion, termination or discipline of employees.

Which disclosures are Protected Disclosures?

An Eligible Disclosure made by an Eligible Whistleblower may attract certain protections under the New Zealand General Whistleblower Regime as described further below.

An Eligible Whistleblower may disclose information in accordance with these Procedures and the Protected Disclosures Act if:

- the information is about serious wrongdoing in or by one or more of the NZ Subsidiary Companies, or any of their related bodies corporate; and
- the Eligible Whistleblower believes on reasonable grounds that the information is true or is likely to be true (even if this belief is mistaken); and
- the Eligible Whistleblower substantially complies with the requirements of the Protected Disclosures Act, even if they do not technically comply; and
- the Eligible Whistleblower wishes to disclose the information so that the serious wrongdoing can be investigated; and
- the Eligible Whistleblower wishes the disclosure to be protected under these Procedures and the Protected Disclosures Act even if they do not expressly refer to the Protected Disclosures Act (together, **Protected Disclosures**).

What is serious wrongdoing?

Serious Wrongdoing includes:

- an offence;
- a serious risk to:
    - public health
    - public safety
    - the health or safety of any individual, or
    - the environment;
- a serious risk to the maintenance of the law, including the prevention, investigation and detection of offences and the right to a fair trial;
- an unlawful, corrupt or irregular use of public funds or public resources; and
- oppressive, unlawfully discriminatory, or grossly negligent conduct or gross mismanagement by
    - a public sector employee, or
    - a person performing a function or duty or exercising a power on behalf of a public sector organisation (the government).

While there are many examples of serious wrongdoing that qualify for protection under the Protected Disclosures Act, serious wrongdoing that should also be reported under the Policy may also include:

- unethical behavior that breaches the NZ Subsidiary Companies key policies, including a breach of the Policy;
- unpermitted use of the NZ Subsidiary Companies funds and resources;
- unlawful, fraudulent or corrupt behaviour including theft, drug sale or use, violence or intimidation, criminal damage to property or other breaches of law; or

- behaviour that may cause the NZ Subsidiary Companies serious financial loss, damage the reputation of the NZ Subsidiary Companies, or otherwise be seriously detrimental to the NZ Subsidiary Companies' interests.

What protections apply?

The key protections available to Eligible Whistleblowers under the New Zealand General Whistleblower Regime include:

1. Confidentiality and Anonymity

Every person to whom a Protected Disclosure is made or referred must use his or her best endeavours not to disclose information that might identify the Eligible Whistleblower who made the Protected Disclosure unless:

- the Eligible Whistleblower consents in writing to the disclosure of that information; or
- the person who has acquired knowledge of the Protected Disclosure reasonably believes that disclosure of identifying information is essential to: (a) the effective investigation of the allegations in the Protected Disclosure; (b) prevent serious risk to public health or public safety or the environment; or (c) the principles of natural justice.

A request for information under the *Official Information Act 1982* or under the *Local Government Official Information and Meetings Act 1987* may be refused, as contrary to the Protected Disclosures Act, if it might identify an Eligible Whistleblower who has made a Protected Disclosure.

2. Immunity from civil and criminal proceedings

An Eligible Whistleblower who makes a Protected Disclosure of information or refers a Protected Disclosure of information to an appropriate authority for investigation, will not be liable to any civil or criminal proceeding or to any disciplinary proceeding by reason of having made or referred that disclosure of information. This protection applies despite any prohibition of, or restriction on, the disclosure of information under any enactment, rule of law, contract, oath or practice.

4. Personal grievance

A personal grievance, as defined in the *Employment Relations Act 2000,* is a type of complaint that an employee can bring against a current or former employer. An employee may raise a personal grievance claim if they believe that their employer has acted unfairly or unreasonably towards them.

Where an Eligible Whistleblower who makes a Protected Disclosure of information under the Protected Disclosures Act claims to have suffered retaliatory action from one or more of the NZ Subsidiary Companies or any of their related bodies corporate, that Eligible Whistleblower:

- if the retaliatory action consists of or includes dismissal, may have a personal grievance, because of a claim of unjustifiable dismissal; and
- if that retaliatory action consists of action other than dismissal, or includes an action in addition to dismissal, may have a personal grievance, because the Eligible Whistleblower's employment, or one or more conditions of the Eligible Whistleblower's employment, is or are or was affected to the Eligible Whistleblower's disadvantage by some unjustifiable action by one or more of the NZ Subsidiary Companies or any of their related bodies corporate.

5. Protections extend to volunteers of supporting information

All protections as stated in these Procedures apply, with all necessary modifications, to a person who volunteers supporting information as if the information were a Protected Disclosure of information.

A person volunteers supporting information if the person:

- provides information, in support of a Protected Disclosure of information made by an Eligible Whistleblower, to:
    - a person investigating the disclosure; or
    - the Eligible Whistleblower who made the Protected Disclosure; and
- is an employee of the NZ Subsidiary Company in respect of which the disclosure was made; and
- wishes to provide the supporting information so that the serious wrongdoing can be investigated.

A person does not volunteer supporting information if the person provides the information only after being required to do so under any enactment, rule of law or contract for the purposes of the investigation, or is approached during the course of the investigation by, or on behalf of, the person investigating the matter.

How do I make a protected disclosure?

If you are aware of or reasonably suspect misconduct or an improper state of affairs or circumstances relating to a NZ Subsidiary Company or any of its related bodies corporate, you are encouraged to first attempt to address the issue by disclosing the information to your People and Performance Business Partner, a member of the Legal and Compliance Department, or to the Chief Legal Counsel. You may also make a disclosure through the confidential Ethics Hotline.

You can also make your disclosure to the head or deputy head of a NZ Subsidiary Company in any case.

All of these persons are authorised by each NZ Subsidiary Company to receive such disclosures for the purposes of the New Zealand General Whistleblower Regime and your disclosure will be treated accordingly.

If you choose to make a Protected Disclosure to a person who is an Eligible Recipient but who is **not** one of the nominated persons above, your disclosure may still attract relevant protections under the New Zealand General Whistleblower Regime. However, you are encouraged to bring the matter to the attention of one or more of the persons nominated above so that the NZ Subsidiary Company is in a position to investigate the matter and take appropriate action in accordance with the Procedures and the Policy.

You may also disclose the information to the Appropriate Authority, as defined in the Protected Disclosures Act, at any time.

An Appropriate Authority is any agency that is listed at Schedule 2 of the Protected Disclosures Act and includes:

- the Commissioner of Police;
- the Controller or Auditor-General;
- the Director of the Serious Fraud office;
- the Inspector-General of Intelligence and Security;
- an Ombudsman;
- the Parliamentary Commissioner for the Environment;
- the Independent Police Conduct Authority;
- the Solicitor General;
- the States Services Commissioner; or
- the Health and Disability Commissioner.

An Appropriate Authority also includes the head of every public sector organisation, but does not include a Minister of the Crown or a Member of Parliament.

Any Protected Disclosure will be investigated in conformity with the Policy. The NZ Subsidiary Company is committed to protecting Eligible Whistleblowers who have made Protected Disclosures from retaliatory action. This includes dismissal, injury, demotion or other detrimental alteration of position or duties, discrimination, harassment or intimidation, damage to property, reputation, business or financial position or any other damage, or threats of any of the foregoing, whether to you as the Eligible Whistleblower or to any other third party (together, **detriment** or **detrimental conduct**).

If you are exposed to any kind of detriment as a consequence of making a Protected Disclosure, you have a right to bring civil or criminal proceedings, or proceedings for civil penalties, against the person or persons causing the detriment (**Detrimental Party**). The court may:

- grant an injunction to prevent, stop or remedy the effects of the detrimental conduct;

- order the Detrimental Party to compensate you or any affected third party for loss, damage or injury suffered as a result of the detrimental conduct;
- order the Detrimental Party to apologise to you or any affected third party;
- where you have been terminated from your position, order the reinstatement of your position or one at a comparable level; or
- order that additional damages be paid to you or any affected third party.

If you choose to seek compensation for breach of the protections available under the New Zealand General Whistleblower Regime in a court, you will generally not have to pay costs unless you have instituted the proceedings unreasonably.

How will my protected disclosure be investigated?

Within 20 working days of receiving a Protected Disclosure, the NZ Subsidiary Company will:

- Acknowledge receipt of your disclosure;
- Consider whether it warrants investigation;
- Check with you whether you have made the disclosure to anyone else; and
- Deal with the matter by doing one or more of the following:
    - investigating the disclosure;
    - addressing any serious wrongdoing by acting or recommending action;
    - referring the disclosure elsewhere; and/or
    - deciding that no action is required.

The NZ Subsidiary Company will inform you, with reasons, what it has done or is doing to deal with the matter. When it is impracticable to complete all these actions within 20 working days, the NZ Subsidiary Company will commence the process, inform you of a timeframe within which it expects to deal with the matter and keep you updated

If the NZ Subsidiary Company decides that no action is required, it will inform you of that decision, with reasons. Reasons may include that:

- it does not consider you meet the requirements of the Protected Disclosures Act to be an employee that has made a Protected Disclosure about Serious Wrongdoing;
- the length of time since the alleged wrongdoing makes an investigation impractical or undesirable; or
- the matter is better addressed by other means.

Fair treatment of parties involved in disclosures

You, as well as any other employees who are mentioned in the Protected Disclosure, will be treated fairly and you will be protected from detriment under the New Zealand General Whistleblower Regime as adopted by these Procedures. You will not, however, be entitled to immunity from

prosecution or other disciplinary action for any misconduct in which you were involved simply because you reported it.

Further information available about these Procedures

This Policy is publicly available on the James Hardie Industries plc Investor Relations website and can also be accessed through the Hardie People Policies SharePoint page. Please contact your People and Performance Business Partner, a member of the Legal and Compliance Department, or the Chief Legal Counsel, if you have any questions about these Procedures or the Policy.

APPENDIX III

PHILIPPINE WHISTLEBLOWER PROCEDURES

James Hardie Philippines Inc (**JHP**) has adopted these Philippine Whistleblower Procedures (**Procedures)** with effect on and from November 2019. These Procedures apply to officers, employees and other eligible whistleblowers of JHP and any Philippine incorporated company forming part of the James Hardie group. JHP and any of its Philippine incorporated companies are referred to in this policy collectively as **the Philippine Subsidiary Companies** and each individually as a **Philippine Subsidiary Company**. These Procedures set out and detail the available "whistleblower" protections under the Revised Corporation Code of the Philippines (Republic Act No. 11232) (**Philippines General Whistleblower Regime)**.

These Procedures contains a general description of the operation of the relevant provisions of the Revised Corporation Code of the Philippines (Republic Act No. 11232). The available protections vary according to the circumstances and subject matter of the contemplated disclosure. If you are in any doubt about how any aspect of these Procedures or the available protections may apply to you, you should seek your own legal advice.

You should read these Procedures in conjunction with the Policy that applies to all James Hardie group entities, including the Philippine Subsidiary Companies. These Procedures supplement the Policy insofar as it applies to the Philippine Subsidiary Companies.

To be protected under these Whistleblower Procedures, an individual must first fall within a certain class of persons as outlined below (**Eligible Whistleblower**). Eligible Whistleblowers are **not** required to identify themselves when making a disclosure and will be eligible for protection in respect of eligible disclosures even if they make the disclosure anonymously. However, the Philippine Subsidiary Companies are no longer accountable for maintaining anonymity where the Whistleblower has disclosed the matter to non-eligible recipients.

Who is an Eligible Whistleblower?

You will be an Eligible Whistleblower if you are or were an:

- individual doing work for or on behalf of a Philippine Subsidiary Company;
- individual who supplies services or goods on a paid or unpaid basis to a Philippine Subsidiary Company; or
- employee of a person supplying services or goods on a paid or unpaid basis to a Philippine Subsidiary Company.

What are Eligible Disclosures?

To be eligible for protection, the Eligible Whistleblower must disclose information that they have reasonable grounds to suspect concerns misconduct or an improper state of affairs or

circumstances in relation to one or more of the Philippine Subsidiary Companies or any of their related bodies corporate (**Eligible Disclosures**). Eligible Disclosures include, but are not limited to:

- violation of the Philippine Subsidiary Company's policy against corrupt practices;
- misuse or misappropriation of the Philippine Subsidiary Company's assets;
- fraudulent reporting or accounting practice;
- violation of the Revised Corporation Code of the Philippines (Republic Act No. 11232);
- conflict of interest situation;
- any conduct that poses a serious risk to public safety, health, or the environment;
- any ethical or illegal conduct; or
- any other conduct similar or related to the foregoing.

An Eligible Whistleblower who is aware or becomes aware of any Eligible Disclosure has a responsibility to disclose the same. Deliberate failure to do so may subject the Eligible Whistleblower to appropriate disciplinary action. In the case of third-party providers, such deliberate failure to disclose may result to loss of accreditation as service provider of the Philippine Subsidiary Company.

What about personal work-related grievances?

Except in the limited circumstances defined below, personal work-related grievances are **not** protected under the Philippines General Whistleblower Regime. Such grievances include matters which relate to an individual's current or former employment and which do not concern an allegation of detriment caused to the individual related to disclosures protected by these Procedures, or which do not have significant implications for a Philippine Subsidiary Company or for James Hardie Industries plc.

Examples of personal work-related grievances include interpersonal conflicts between employees and decisions relating to the engagement, transfer, promotion, suspension, demotion, termination or discipline of employees.

Which disclosures are Protected Disclosures?

To be protected, the disclosure must be eligible (see *Eligible Disclosures*), and disclosed by the Eligible Whistleblower (whether verbally, in writing, or via electronic mail) in good faith to the following persons (together, the **Eligible Recipients**):

- an officer or senior manager of a Philippine Subsidiary Company or of a related body corporate;
- an auditor or member of an audit team conducting an audit on a Philippine Subsidiary Company or a related body corporate;
- an actuary of a Philippine Subsidiary Company or of a related body corporate;
- a person or body prescribed by regulation; or

- a person authorized by a Philippine Subsidiary Company to receive such disclosures.

The Eligible Whistleblower may also make a disclosure through the confidential Ethics Hotline. Any Protected Disclosure will be investigated in conformity with the Policy. A whistleblower who is found to have made malicious and false allegations shall be subject to appropriate disciplinary or legal action.

What protections apply?

The key protections available to Eligible Whistleblowers include:

1. Confidentiality and Anonymity

If the Eligible Whistleblower makes a Protected Disclosure, the identity of the whistleblower, as well as any information that is likely to identify the whistleblower, must be kept confidential by the recipient. There are a limited number of circumstances where the identity of the whistleblower and/or any related information will not remain confidential, namely where the information is disclosed by the whistleblower (a) to a non-eligible recipient or (b) in court where the Eligible Whistleblower is required to stand as a witness in court.

Information that is likely to identify the Eligible Whistleblower may also be disclosed where the disclosure is necessary to investigate the misconduct or improper state of affairs to which the disclosure relates, and the disclosing recipient takes reasonable steps to reduce the risk of the Eligible Whistleblower being identified.

2. Protection from Administrative Proceedings

If you make a Protected Disclosure, you will generally be protected from administrative liability as a result of having made the disclosure, including disciplinary, contractual or other action such as termination of your employment contract where your disclosure would otherwise have constituted a breach of that contract. However, this does not prevent you being subject to civil, criminal or administrative liability or action in respect of your own conduct revealed by the disclosure.

3. Protection from Retaliation

Any person who, knowingly and with intent to retaliate, commits acts detrimental to an Eligible Whistleblower, such as interfering with his/her lawful employment or livelihood, shall, at the discretion of the court, be punished with a fine ranging from One hundred thousand pesos (P100,000.00) to one million pesos (P1,000,000.00).

If the Eligible Whistleblower believes that he/she is being retaliated against for reporting suspected misconduct, the whistleblower is encouraged to report such matter to (i) the Eligible Recipients or (ii) the Ethics Hotline.

Fair treatment of parties involved in disclosures

The Eligible Whistleblower, as well as any other employees or related parties who are mentioned in the Protected Disclosure, will be treated fairly and will be protected from detriment under these Procedures. The Eligible Whistleblower will not, however, be entitled to immunity from prosecution or other disciplinary action for any misconduct in which you were involved simply because you reported it.

Further information available about these Procedures

This Policy is publicly available on the James Hardie Industries plc Investor Relations website and can also be accessed through the Hardie People Policies SharePoint page. Please contact your People and Performance Business Partner, a member of the Legal and Compliance Department, or the Chief Legal Counsel, if you have any questions about these Procedures or the Policy.

APPENDIX IV

SPECIAL REPORTING REQUIREMENTS FOR EMPLOYEES IN GERMANY

In addition to the information outlined in this Policy, employees who are employed in Germany should also note the following specifics / requirements regarding the use of the Ethics Hotline:

ACTIVITIES AND ISSUES TO BE REPORTED

In Germany, there are limitations as to the issues that may be reported. Only serious issues (**Serious Issues**) may be communicated through the Ethics Hotline, as detailed below. The Ethics Hotline is not intended for the reporting of **violations of the Company's Global Code of Business Conduct** unless it is a Serious Issue and falls into one of the following categories:

- accounting or audit irregularities;
- antitrust or competition or trade practice violations (e.g., unauthorized discounts, cartel conduct such as price fixing, market sharing etc.);
- breach of the Global Code of Business Conduct;
- breach of any applicable law or regulation;
- bribes or kickbacks;
- corporate espionage or sabotage;
- conflicts of interest;
- unauthorized disclosure of proprietary information and/or personal data;
- employment issues (e.g., discrimination/unlawful harassment, drug abuse, etc.);
- environmental, health and safety issues;
- falsification of Company records;
- fraud or theft of cash or Company property;
- insider trading; and
- other serious misconduct, dishonest or illegal activity.

In particular, the private life of other employees should not be made subject to a report via the Ethics Hotline.

If you have concerns you would like to report that cannot be reported through the Ethics Hotline, please address the issue with your supervisor, a representative in the Human Resources Department, an attorney or other representative within the Legal and Compliance Department, or directly with the Chief Legal Counsel.

ANONYMITY AND CONFIDENTIALITY

If you are in **Germany**, you will only be able to report anonymously through the Ethics Hotline. We have instructed the third-party provider of the Ethics Hotline not to record your name or other identifying details you might have provided.

If you would like to disclose your identity when communicating your concern, please do so through other communication channels (e.g. by contacting a representative in the Human Resources Department or an attorney or other representative within the Legal and Compliance Department).

APPENDIX V

SPECIAL REPORTING REQUIREMENTS FOR EMPLOYEES IN THE UNITED KINGDOM

ANONYMITY AND CONFIDENTIALITY

You are under no obligation to identify yourself when making a report, and can, if you prefer, report anonymously. However, it is important to understand that it may be more difficult for you to qualify for whistleblower protections (see below) if there is no record of the report linking to you as an individual.

You are also under no obligation to disclose the wrongdoing of others, although we encourage you to do so where that wrongdoing is a Serious Issue and falls into one of the following categories:

- accounting or audit irregularities;
- antitrust or competition or trade practice violations (e.g., unauthorized discounts, cartel conduct such as price fixing, market sharing etc.);
- breach of the Global Code of Business Conduct;
- breach of any applicable law or regulation;
- bribes or kickbacks;
- corporate espionage or sabotage;
- conflicts of interest;
- unauthorized disclosure of proprietary information and/or personal data;
- employment issues (e.g., discrimination/unlawful harassment, drug abuse, etc.);
- environmental, health and safety issues;
- falsification of Company records;
- fraud or theft of cash or Company property;
- insider trading; and
- other misconduct, dishonest or illegal activity.

The law recognizes that you have a right to disclose wrongdoing even where you are bound by a duty of confidentiality, either to the Company (including your employing entity) or a third party.

MAKING A QUALIFYING DISCLOSURE AS A WHISTLEBLOWER

UK law protects whistleblowers who make 'qualifying disclosures'. If you make a qualifying disclosure, you will be automatically be protected as a whistleblower - there is no need for you to do anything to apply for this status. In order to for your report to be a qualifying disclosure, it must satisfy the following conditions:

i. You must actually disclose information (a mere threat to disclose information, or an indication that information might later be disclosed, cannot qualify). However, the means of communicating the disclosure (written, verbal, telephone etc.) is not relevant.

ii. The subject matter of the report must relate to one of six types of relevant failure, which are as follows:

   a. a criminal offence;
   b. a breach of any legal obligation;
   c. a miscarriage of justice;
   d. danger to the health and safety of any individual;
   e. damage to the environment; or
   f. the deliberate concealing of information about any of the above.

   Therefore, a breach of Company policy which is not a breach of the law may not qualify, unless it satisfies one of the other criteria (e.g. it represents a danger to an individual's health and safety).

iii. You must have a reasonable belief that the report relates to one of the six types of relevant failure. You do not have to demonstrate that any of the facts or allegations in the report are actually true, or even that the facts or allegations legally constitute one of the types of relevant failure, provided you have an honest subjective belief that one of the types of relevant failure had occurred.

iv. You must have a reasonable belief that the disclosure is in the public interest.

LEGAL PROTECTION FOR WHISTLEBLOWERS

If you make a qualifying disclosure, you benefit from certain protections for whistleblowers. Most importantly, you have the right not to be subject to any detriment on the grounds of having made that disclosure.

It is important to note that the Company encourages reports regardless of whether or not they are qualifying disclosures. If you have any concerns or questions, please contact a representative in the Human Resources Department, an attorney or other representative within the Legal and Compliance Department or directly with the Company's Chief Legal Counsel.

APPENDIX VI

SPECIAL REPORTING REQUIREMENTS FOR EMPLOYEES IN SPAIN

In addition to the information outlined in this Policy, employees who are employed in Spain should also note the following specifics / requirements regarding the use of the Ethics Hotline:

ACTIVITIES AND ISSUES TO BE REPORTED

In Spain, there are limitations as to the issues that may be reported. Only issues that imply a **breach of general or sectorial provisions** may be communicated through the Ethics Hotline.

The Ethics Hotline is in particular not intended for the reporting of **violations of the Company's Global Code of Business Conduct** unless these also fall into the description provided above. In particular, the private life of other employees should not be made subject to a report via the Ethics Hotline.

If you have concerns you would like to report that cannot be reported through the Ethics Hotline, please address the issue with your supervisor, a representative in the Human Resources Department, an attorney or other representative within the Legal and Compliance Department or directly with the Company's Chief Legal Counsel.

INVESTIGATION PROCESS

If you are in **Spain**, your report shall be examined only by professionals (whether working for the group or outsourced staff) working in the area, internal audit and compliance. No other business professionals (e.g. HR, Legal) will be involved except when it may be required for adopting disciplinary measures or for handling litigation matters.

RECORDS RETENTION

In **Spain**, the data of the reporting person, of the employees and of the third parties involved shall be retained only for the time that is strictly required to decide whether an investigation shall be opened. In any event, after three months from the date of registration this data shall be deleted from the Ethics Hotline databases (except to demonstrate, within the context of the corporate compliance and crime prevention scheme, that the hotline is working properly). Notwithstanding the foregoing, the data may be transferred to the databases held by the Board or committee undertaking the investigation (if the opening of the investigation has been decided). All data related to non-opened investigations shall be fully anonymized or, else, deleted.

APPENDIX VII

SPECIAL REPORTING REQUIREMENTS FOR EMPLOYEES IN THE NETHERLANDS

In addition to the information outlined in this Policy, employees who are employed in the Netherlands should also note the following specifics / requirements regarding the use of the Ethics Hotline:

ACTIVITIES AND ISSUES TO BE REPORTED

As set out in the Policy, whenever you have a concern about a party's ethical or business conduct, you should first attempt to address the issue with your supervisor, a representative in the Human Resources Department, an attorney or other representative within the Legal and Compliance Department or directly with the Company's Chief Legal Officer. You can do this in writing, by means of a meeting in the office or a phone call.

In addition, in the Netherlands, all (suspicions of) misconduct may be reported through the Ethics Hotline, i.e., if you believe that the Company or someone acting on behalf of the Company has done, is doing, or may be about to do something that significantly violates the law or Company policies or commits a serious act of misconduct. This includes violation of EU-legislation, a danger to public health, to the safety of persons, to the environment or to the proper functioning of the public service or an enterprise as a result of improper acts or omissions.

ANONYMITY AND CONFIDENTIALITY

If you make a report through the Ethics Hotline, the report will be registered by means of:

(a) a recording of the conversation in a durable and retrievable form; or
(b) a complete and accurate written record of the conversation.

Recording of the conversation as set out under (a) will only take place upon your prior consent. You will be provided the opportunity to verify, correct and sign for approval the written record of the conversation as set out under (b).

EXTERNAL REPORTING

If you are in the Netherlands, you have the possibility to address the external Whistleblowers House (*Huis voor Klokkenluiders,* www.huisvoorklokkenluiders.nl):

- to report a (suspicion of a) misconduct for investigation
- to request an investigation in relation to how the employer has dealt with an internal report of (suspicion of) misconduct
- to ask for information or advice in relation to report a (suspicion of a) misconduct.

In the event of suspected wrongdoing, Employees also have the possibility to request of the Whistleblowers House confidential, independent and free of charge advice on how to act.

RECORDS RETENTION

In the Netherlands, the data of the reporting person, of the employees and of the third parties involved shall be retained only for the time that is strictly required to decide whether an investigation shall be opened. Once the investigation has been completed, the relevant data shall be deleted from the Ethics Hotline databases unless it is necessary to store the data longer, in particular in case of ongoing legal proceedings. All data related to non-opened investigations shall be fully anonymized or, else, deleted.

APPENDIX VIII

SPECIAL REPORTING REQUIREMENTS FOR EMPLOYEES IN ITALY

ANONYMITY AND CONFIDENTIALITY

You are under no obligation to identify yourself when making a report, and can, if you prefer, report anonymously. However, it is important to understand that it may be more difficult for you to qualify for whistleblower protections if there is no record of the report linking to you as an individual.

Therefore, your report should not be anonymous and the Company invites you to identify yourself to allow your effective protection against any retaliation. This will also allow a better management of the file if further information would be necessary.

ACTIVITIES AND ISSUES TO BE REPORTED

Reports must be detailed and based on precise and consistent factual elements. You must provide all possible elements in your knowledge to enable the persons responsible to carry out the necessary and appropriate checks and inspections to confirm the validity of the facts reported, although it is not essential that the reporter has sufficient evidence to prove the fact reported.

LEGAL PROTECTION FOR WHISTLEBLOWERS

If you make a qualifying disclosure, you benefit from certain protections for whistleblowers. Most importantly:

- you have the right not to be subject to any detriment on the grounds of having made that disclosure;
- your identity will be protected both in the disciplinary and in the criminal proceedings.

It is important to note that the Company encourages reports regardless of whether or not they are qualifying disclosures. If you have any concerns or questions, please contact a representative in the Human Resources Department, an attorney or other representative within the Legal and Compliance Department or directly with the Company's Chief Legal Counsel.

APPENDIX IX

SPECIAL REPORTING REQUIREMENTS IN FRANCE

In addition to the information outlined in this Policy, employees who are employed in France should also note the following specifics / requirements regarding the use of the Ethics Hotline:

In addition to the information outlined in this Policy, the persons eligible to make reports in France (see section "Who can report") should also note the following specifics / requirements regarding reporting of facts covered by this Appendix.

WHO CAN REPORT

The following individuals are entitled to make a report, acting in good faith and without having direct financial compensation:

- employees and former employees, where the information was obtained in the course of their employment;
- job applicants, where the information was obtained in the course of their application;
- shareholders, partners and holders of voting rights in the entity's general meeting;
- external and occasional collaborators;
- members of the administrative, management or supervisory body of the entity;
- co-contractors and sub-contractors of the entity, members of the administrative, management or supervisory bodies of these co-contractors and subcontractors, as well as members of their staff.

ACTIVITIES AND ISSUES TO BE REPORTED

Without limiting the scope of elements that can be reported per this Policy, it is specified that the following matters may in any case be reported in France:

- a crime or a misdemeanor;
- a violation or an attempt to conceal a violation of an international commitment duly ratified or approved by France, or of a unilateral act of an international organization adopted on the basis of such a commitment;
- a violation or an attempt to conceal a violation of the law of the European Union, or of French law or of French regulation;
- a threat or harm to the general interest.

ISSUES THAT CANNOT BE REPORTED

Information, facts or documents the disclosure of which is prohibited by the provisions relating to national defense secrecy, medical confidentiality, the secrecy of judicial deliberations, the secrecy of judicial investigations or inquiries, or the attorney-client privilege, cannot be reported under this Policy.

CONDITIONS FOR REPORTING

Prior to making any report, the Reporter is informed in accordance with Article 13 of the GDPR of the conditions of the processing of his/her data when using the Ethics Hotline.

The Reporter is informed that the Ethics Hotline is not the exclusive mean available to make a report and that other alternative measures may also be used such as the hierarchical reporting.

The Reporter is also informed that an abusive use of the Ethics Hotline may be subject to disciplinary sanctions or other judicial proceedings. On the contrary, the use of the Ethics Hotline in good faith will not be sanctioned even if the reported facts are finally considered as incorrect or if a closure of the reporting is decided.

Oral reporting requirements

The report can be addressed in writing or orally.

If orally, it is possible to report by telephone or any other voicemail device and, at the reporter's request, by videoconference or physical meeting organized within 20 days from the request's reception.

Any report made orally shall be recorded as follows:

- when collected, with the consent of the reporter, on a recorded telephone line or other recorded voice mail system, either by recording the conversation on a durable and recoverable medium or by transcribing the conversation in full;
- when taken over an unrecorded telephone line or other unrecorded voice mail system, by drafting accurate minutes of the conversation;
- when taken in a videoconference or physical meeting, by making, with the consent of the reporter, either a recording of the conversation on a durable and retrievable medium or by drafting accurate minutes of the conversation.

The reporter must ensure to only report factual information that presents a direct link with the subject of the report. Any data of the report considered as not falling within the scope of the issues that can be reported will be deleted or anonymized without undue delay.

Acknowledgment of receipt of a report

The reporter is informed in writing of the receipt of the report within 7 working days of its receipt.

Admissibility of the report

The admissibility of all reports is verified by the first recipient of the report based on the following conditions:

- the reported facts meet the above-mentioned scope (see section "Activities and issues that can be reported");
- the reported facts do not concern any of the above-mentioned exclusions (see section "Issues that cannot be reported");
- the reporter is entitled to make reports under this Policy (see section "Who can report");

To this end, complementary information may be requested from the reporter.

The Company will ensure that only the relevant information necessary for the purpose of the reports is collected and kept. Therefore, special categories of data or data relating to criminal convictions and offenses may be collected to the extent allowed by applicable data protection law or necessary to establish, exercise or defend a right in justice.

Outcomes for non-admissible reports

If considered non-admissible, the reporter is informed of the reasons why the report was considered non-admissible. Non-admissible reports will be deleted or anonymized as detailed below (see section "Closure of the report").

Anonymous reports

The Ethics Hotline should not be used for anonymous reporting. This being said, by exception, an employee can stay anonymous if the seriousness of mentioned facts is established and the factual elements to support the allegations are sufficiently detailed. In addition, the processing of such alert must be done with peculiar caution, such as a preliminary examination of the need to communicate the report, by its first recipient.

Anonymous reports that are deemed non-admissible are treated as non-admissible reports, per this Appendix. Anonymous reports that are deemed admissible are treated as all other reports, per this Appendix.

External reporting channels

Depending on the issue reported, reporters can also address their report to external authorities (e.g., the French Data Protection Supervisory Authority for non-compliance with data protection law or cybersecurity issues) or make their report public under conditions set out by French law. Further information on such reporting and its related conditions can be found in the Decree of 3 October 2022 (No. 2022-1284) as modified, as the case may be.

INVESTIGATION PROCESS

The section "Investigation process" applies, as relevant, to all reports received by the French entity of the Company.

Processing of a report

Information needed to assess the reported information may be sought from the reporter at any time during the processing of the report by the persons in charge of investigating the report.

The Head of Legal Europe or his/her delegate shall, within a reasonable period of time not exceeding 3 months from the acknowledgement of receipt of the report or, if no acknowledgement is received, 3 months from the expiration of a period of 7 working days following the report, provide the reporter with written information on the measures envisaged or taken to assess the accuracy of the reported information and, where appropriate, to remedy the subject-matter of the report, as well as the reasons for the measures taken.

Closure of the report

The reporter is informed in writing of the closure of the report when the remediation measures are adopted, or when the reported facts do not fall within the scope of the Ethics Hotline, are incorrect or not substantiated.

If the reported facts do not fall within the scope of the Ethics Hotline, the personal data included in the report will be immediately deleted or anonymized.

If the reported facts are incorrect or not substantiated so that a closure of the report is decided, the personal data included in the report will be deleted or anonymized within a period of 2 months following the date of completion of the report verification.

If disciplinary or litigation proceedings are initiated against the persons designated in the report or the author of an abusive report, the personal data included in the report will be kept until the end of the proceedings or, in intermediate archiving, until the end of the statute of limitation period applicable to appeal against the decision.

Requirements regarding the recipients of reports

The persons and services designated to receive and verify reports shall, by virtue of their position or status, have the competence, authority and means to perform their duties. All tasks pertaining to receipt and verification of reports will be carried out with impartiality and ensuring the confidentiality of the information.

If such recipients are located outside the EU in a country which does not benefit from an adequacy decision of the EU Commission, the transfer is protected by the implementation of the relevant EU Commission Standard Contractual Clauses in their version 2021 and supplemented as needed by additional contractual, organizational and security measures to ensure the legality of the transfer. A copy of the transfer mechanism may be obtained at the following electronic address: dpo@jameshardie.com.

ANONYMITY AND CONFIDENTIALITY

The integrity and confidentiality of the information collected in a report, including the identity of the author of the report, the individuals designated in it and any third parties, as well as any information collected during the process shall be ensured.

It is forbidden to give any access to that information to persons that are not designated to receive or verify the reports under the Policy and this Appendix. If the report is addressed to an unauthorized person or service, this recipient transmits it immediately to an authorized person or service mentioned in this Policy.

The information likely to identify the reporter may only be disclosed with his or her consent. It may, however, be communicated to the judicial authority, if the person responsible for collecting or processing the alerts is required to report the facts to such authority. The reporter is then notified of such disclosure unless this notification would compromise the judicial proceedings.

In the same manner, the information likely to identify the person subject to the report may not be disclosed, except to the judicial authority, only when the report has been established as being grounded.

The person designated in the report will only be informed thereof where such information complied with the requirements relating to confidentiality set out above and to the extent the entity has not resolved to delay such information in compliance with the applicable data privacy laws and regulations.

Provided that the information does not seriously compromise the performance of the objectives of the processing, the Head of Legal Europe will inform the individual designated in the report, so that such individual is informed of the processing activity and can notably oppose to the processing of his/her data. Otherwise, such information will be deferred to prevent notably the risk of evidence destructions. For the sake of clarity, this information is limited to the information not protected by confidentiality and will include the modalities of his/her right of access, opposition and rectification.

NO RETALIATION

Without limitation to the generality of the protections provided in the Policy, it is specified that no retaliation, threats or attempts to take such measures against any person who has in good faith made reports in compliance with this Policy and its Appendix for France. Examples of prohibited measures can be found in article 10-1 of the of law of 9 December 2016 (No. 2016-1691), as modified.

It is also prohibited to retaliate against:

- any person helping the reporter to disclose facts;

- any person linked to the reporter who risks being subject to one of the retaliation measures, in the context of their professional activities by their employer, their client or the recipient of their services;
- any person controlled by the reporter, for which he works or with which he is linked in a professional context.

It is also specified that employees will not be retaliated against for not using this Ethics Hotline.

DATA PRIVACY RULES SPECIFIC FOR FRANCE

The Company will respect the applicable data privacy laws and regulations in France, including guidelines issued by the French Data Protection Authority (CNIL) on whistleblowing schemes (in particular the "*Délibération n° 2019-139 du 18 juillet 2019 portant adoption d'un référentiel relatif aux traitements de données à caractère personnel destinés à la mise en œuvre d'un dispositif d'alertes professionnelles*").

More specifically:

- The Controller of the processing resulting from the Ethics Hotline is the French entity of the Company, James Hardie Bâtiment SAS, 1 rue de l'Union, 92500 Rueil-Malmaison, France, info@jameshardie.fr.

- The purpose of the processing is to manage reports provided through the Ethics Hotline, notifying potential misconduct in violation of Company policies or noncompliance with applicable laws and regulations.
- The Company relies on its legitimate interest to ensure that its business is carried out in compliance with the applicable laws and in an ethical manner.

- Data subjects have the right to lodge a complaint to the French Data Protection Supervisory Authority (the CNIL, www.cnil.fr). They also have the right to object to the processing of their data in the conditions set forth in Article 21 of the GDPR, the right of access in the conditions of Article 15 of the GDPR, rectify and delete their data in the conditions of Articles 16 and 17 of the GDPR, the right to restriction in the conditions of Article 18 of the GDPR.

If you are an employee of the Company, for further information regarding how to exercise such rights, the data recipients involved, and the conditions of transfers please consult Appendix XII – Privacy Notice European Citizen Employee Data below.

APPENDIX X

SPECIAL REPORTING REQUIREMENTS FOR EMPLOYEES IN DENMARK

In addition to the information outlined in this Policy, employees who are employed in Denmark should also note the following specifics / requirements regarding the use of the Ethics Hotline:

ACTIVITIES AND ISSUES TO BE REPORTED

In Denmark, there are limitations as to the issues that may be reported. Only instances of serious misconduct (or reasonably suspected serious misconduct) that may have an impact on the Company as a whole or that may have a significant impact on the life or health of any individual may be reported through the Ethics Hotline.

Such instances include, but are not limited to, bribery, fraud, forgery, sexual harassment, severe personal conflicts, environmental pollution, serious non-compliance with health and safety regulations, etc.

Generally, individuals' minor misconduct within the workplace (such as work attire, sickness absence, misuse of office supplies, and other minor non-compliant behaviours with Company policies on conduct, etc.) may not be reported via the Ethics Hotline. In particular, the private lives of other employees should not be made subject to a report via the Ethics Hotline.

If you have any concerns you would like to share that cannot be reported through the Ethics Hotline, please address the issue with your supervisor or a representative in the Human Resources Department.

ANONYMITY AND CONFIDENTIALITY

During the course of an investigation, the Company and Navex will keep your identity confidential to the widest extent possible and in accordance with Danish law. Information about the subject of the reported issue will be processed in compliance with the subject's mandatory legal rights, including applicable data protection regulation.

APPENDIX XI

SPECIAL REPORTING REQUIREMENTS FOR EMPLOYEES IN IRELAND

The Company reserves the right to make any changes and amendments to this Appendix that it considers necessary in its sole discretion.

In addition to the Company's Ethics Hotline, this Appendix covers "workers" in Ireland who acquire information, on relevant wrongdoings (see matters covered below) in a work-related context, who make a report via their local in-country reporting channel.

WHO CAN MAKE A PROTECTED DISCLOSURE

"Workers" includes an individual who is or was an employee; contractors; sub-contractors; volunteers; paid or unpaid trainees; agency workers where the worker is supplied by a third person to the Company; self-employed individuals; shareholders; members of the company's administrative, management and supervisory bodies (including non-executive members); anyone working under the supervision and direction of contractors, subcontractors and suppliers; and anyone in any of the above categories whose work-based relationship with the Company is yet to begin or has ended (collectively described as '**workers**' in this Appendix).

ANONYMITY AND CONFIDENTIALITY

We hope that workers will feel able to voice whistleblowing concerns openly. However, if you want to raise your concern confidentially, the Company is committed to protecting your identity and ensuring that relevant disclosures are treated in confidence. The focus will be on the wrongdoing rather than the person making the disclosure.

This means that, where possible:

- no unauthorised staff member is allowed access to information held within the protected disclosure;
- the identity of the reporting person, together with any other information from which their identity may be directly or indirectly deduced, will be kept confidential and protected and will not be disclosed, without the individual's consent, to anyone beyond authorised members of staff who are competent to receive, follow-up or provide feedback on a report;
- the identity of an individual who makes a report may be disclosed in very limited circumstances permitted by law.

However, there are circumstances, where confidentiality cannot be maintained, particularly in a situation where the worker is participating in an investigation into the matter being disclosed. Should such a situation arise, every effort will be made to inform the worker that his/her identity may be disclosed.

A concern may also be raised anonymously. However, on a practical level it may be difficult to investigate such a concern and it may be more difficult for you to qualify for whistleblower protections if there is no report linking to you as an individual. Accordingly, workers are encouraged to put their names to allegations, with the Company's assurance of confidentiality where possible, in order to facilitate appropriate follow-up. This will make it easier for us to assess the disclosure and take appropriate action including an investigation if necessary.

INVESTIGATION INTO THE DISCLOSURE

It is possible that in the course of an investigation, you may be asked to clarify certain matters. For the purposes of confidentiality, such a meeting can take place off site and you can choose whether or not to be accompanied by a colleague.

MAKING A PROTECTED DISCLOSURE AS A WHISTLEBLOWER

Irish law protects whistleblowers who make "protected disclosures".

A protected disclosure is a disclosure of information which, in the reasonable belief of the worker concerned, tends to show one or more relevant wrongdoings (see below). If you make a '**protected disclosure**' you will be automatically protected as a whistleblower – there is no need for you to do anything to apply for this status. In order for your report to be a protected disclosure, your disclosure must follow each of the following conditions:

i. The subject matter of the report must relate to a '**relevant wrongdoing**', which in this context is limited to the following:

   a. that an offence has been, is being or is likely to be committed;
   b. that a person has failed, is failing, or likely to fail to comply with any legal obligation (other than one arising under the worker's contract of employment or terms of engagement);
   c. that a miscarriage of justice has occurred, is occurring or is likely to occur;
   d. that the health and safety of any individual has been, is being or is likely to be endangered;
   e. that the environment has been, is being or is likely to be damaged;
   f. that an unlawful or improper use of public money has occurred, is occurring or is likely to occur;
   g. oppression, discrimination, gross negligence or gross mismanagement by or on behalf of a public body;
   h. that a breach has occurred, is occurring or is likely to occur**; or
   i. that information tending to show any matter falling within any of the preceding sections (a) to (h) has been, is being or is likely to be concealed or destroyed or an attempt has been, is being or is likely to be made to conceal or destroy such information.

**Breaches under section (h) above are understood as any acts or omissions that (i) are unlawful and related to the European Union acts and areas falling within the scope of the list detailed below, and (ii) defeat the object or the purpose of the rules in the Union acts and areas falling within the scope of the following list:

- Public procurement;
- Financial services, products and markets, prevention of money laundering and terrorist financing;
- Product safety and compliance;
- Transport safety;
- Protection of the environment;
- Radiation protection and nuclear safety;
- Food and feed safety and animal health and welfare;
- Public health;
- Consumer protection;
- Protection of privacy and personal data and security of network and information systems;
- Breaches affecting the financial interests of the EU;
- Breaches relating to the EU internal market including breaches of –
    - Competition and State aid rules;
    - Rules on corporate tax including any tax arrangements.

ii. You must have a reasonable belief that the report tends to show one or more of the relevant wrongdoings listed above; and

iii. The information that is disclosed must have come to your attention in connection with your employment. However, it is not a protected disclosure if it is your function (or that of the Company) to detect, investigate or prosecute the relevant wrongdoing, and the relevant wrongdoing does not involve an act or omission on the part of the Company.

This Policy should not be used for complaints relating to your own personal circumstances, such as complaints regarding your own contract of employment, duties, terms and conditions of employment, working procedures or working practices. Furthermore, a matter concerning interpersonal grievances exclusively affecting you, namely, grievances about interpersonal conflicts between you and another worker, or a matter concerning a complaint by you to, or about, your employer which concerns you exclusively is also not covered by this Policy. These are grievances, not protected disclosures, and so are processed under the Company's Grievance Policy.

Please note only disclosures concerning the actions falling within the categories outlined above will be eligible for the relevant statutory protection and in order for a disclosure of information to be treated by the Company as a protected disclosure, then it must be reported under this Policy.

LEGAL PROTECTION FOR WHISTLEBLOWERS

A worker who makes a protected disclosure and has a reasonable belief of wrongdoing will not be penalised by the Company, even if the concerns or disclosure turns out to be unfounded.

Penalisation for the purpose of this Policy includes suspension, lay off or dismissal, disciplinary action, demotion, loss of opportunity for promotion or withholding of promotion, transfer of duties, change of location of place of work, reduction in wages or change in working hours, the imposition or administering of any discipline, reprimand or other penalty (including a financial penalty), coercion, intimidation, harassment or ostracism, injury, damage or loss, threat of reprisal, withholding of training, a negative performance assessment or employment reference, failure to convert a temporary employment contract into a permanent one, where the worker had a legitimate expectation that he or she would be offered permanent employment, failure to renew or early termination of a temporary employment contract, harm, including to the worker's reputation, particularly in social media, or financial loss, including loss of business and loss of income, blacklisting on the basis of a sector or industry-wide informal or formal agreement, which may entail that the person will not, in the future, find employment in the sector or industry, early termination or cancellation of a contract for goods or services, cancellation of a licence or permit, psychiatric or medical referrals, discrimination, disadvantage or unfair treatment, threats or unfavourable treatment arising from the disclosure. Workers who penalise, threaten or retaliate against those who have raised concerns under the Policy will be subject to disciplinary action. The Company will take appropriate steps to protect workers who makes a protected disclosure, including taking necessary action, which may include but is not limited to disciplinary action or dismissal, against anyone who is found to be pursuing any form of retaliation or has threatened to do so.

Workers are not expected to prove the truth of an allegation. However, they must have a reasonable belief that there are grounds for their concern. A disclosure that is made without any reasonable belief as to its accuracy, or knowing it to be false, may result in disciplinary action.

If you have any concerns or questions or believe that you are being subjected to penalisation as a result of making a disclosure under this Policy, please contact a representative in the Human Resources Department, an attorney or other representative within the Legal and Compliance Department or directly with the Company's Chief Legal Counsel.

LOCAL REPORTING CHANNEL

The Company considers raising your concern through the Ethics Hotline is the most appropriate and efficient action for you to take. However, as an alternative to the Ethics Hotline outlined above, you may report via the Company's local reporting channel as described in further detail below.

Internal reporting

- The Company's local internal reporting channel for whistleblowing reports is operated locally by the Head of the Dublin Office who has been designated to carry out this function.

You may make your report orally, in writing or in person. In case you choose to make an oral report or report in person, the Head of the Dublin Office (or his/her designee) has been designated to carry out this function and shall either record the conversation or draft a complete and accurate transcript of the conversation. You will be given the opportunity to check, correct and ensure the accuracy of the written transcript of the conversation.

You should make your report as specific as possible and include details such as but not limited to:

- The type of wrongdoing you are reporting;
- Where and when relevant events occurred;
- Who is involved and who has knowledge of the matter you are reporting;
- How the individual or organisation committed the relevant wrongdoing (see section above);
- Any documents or other sources that support the information in your report.

The Head of the Dublin Office will be responsible for:

- Acknowledging receipt of your report within seven days.
- Maintaining communication with you including asking for further information on the report, where necessary.
- Diligently following up/investigating a report to assess the accuracy of the allegations made in the report.
- Providing feedback to you on your report. Feedback will be provided within a reasonable timeframe which will not exceed three months from acknowledgement of receipt of your report.

When a worker makes an internal report, the Company will process any personal data collected in compliance with applicable laws and regulations and in accordance with its Data Protection Policy and Employee Data Privacy Notice (See Appendix XII). Data collected from the point at which an individual makes the report is held securely and accessed by, and disclosed to, only authorised individuals and only for so long as is necessary.

EXTERNAL DISCLOSURES

The aim of this Policy is to provide an avenue within the Company to deal with concerns or disclosures in regard to wrongdoing. We are confident that issues can be dealt with through the Ethics Hotline, or via the local reporting channels.

The Company acknowledges that there may be circumstances where a worker wants to make a disclosure to a competent external authority i.e. the Protected Disclosures Commissioner. It will very rarely, if ever, be appropriate to alert the media. It is important to note, however, that while you need only have a reasonable belief as to wrongdoing to make a disclosure internally, if you

are considering an external disclosure, different and potentially more onerous obligations apply depending on to whom the disclosure is made.

Whistleblowing concerns usually relate to the conduct of employees within the Company, but they may sometimes relate to the actions of a third party, such as a customer, supplier or service provider.

In some circumstances, the law will protect you if you raise the matter with the third party directly. However, we encourage you to report such concerns internally first.

APPENDIX XII

PRIVACY NOTICE EUROPEAN CITIZEN EMPLOYEE DATA

INTRODUCTION AND CONTACT DETAILS

At James Hardie, we are committed to maintaining the accuracy, confidentiality and security of your Personal Data. This Data Privacy Notice describes the Personal Data that James Hardie Industries plc including its subsidiaries and affiliates (hereinafter "James Hardie"), may collect from or about you, how your privacy is safeguarded, how your Personal Data may be used and to whom it may be disclosed.

Please read the following notice carefully to understand our views and practices regarding your Personal Data and how we treat it. The following Data Protection Notice describes the categories of Personal Data we process, how your Personal Data may be processed, for what purposes we may process your data and how your privacy is safeguarded in the course of your work for us.

PRIVACY AND DATA PROTECTION OFFICE AND DATA PROTECTION OFFICERS

James Hardie has established a Privacy and Data Protection Office with data protection experts across the globe. In addition, for Germany, James Hardie has appointed a Data Protection Officer. If you have any questions regarding the processing of your Personal Data or if you believe your privacy rights have been violated, you may contact our global Privacy and Data Protection Office, the local Data Protection Officer (if you reside in Germany) or your local Human Resources department.

Privacy and Data Protection Office	Data Protection Officer Germany
Europe (general)	Germany (only)
Attn: Privacy and Data Protection Office Bennigsen-Platz 1 40474 Düsseldorf Germany Dpo@jameshardie.com	Attn: Data Protection Officer Bennigsen-Platz 1 40474 Düsseldorf Germany datenschutz-fermacell@jameshardie.com

WHO IS THE DATA CONTROLLER

The respective James Hardie entity that employs you is the Data Controller of your Personal Data. In addition, where processing of Personal Data is undertaken by affiliated companies of James Hardie for their own independent purposes, these affiliated companies may be controllers of your

Personal Data as well. The details of those James Hardie companies that process Personal Data as controller are listed in Annex A.

COLLECTION AND USE (PROCESS) OF YOUR PERSONAL DATA

We collect and maintain different types of Personal Data in respect of those individuals who would like to be, are, or were employed by us. "**Personal Data**" is any information that can be used to identify an individual. We may collect and process your Personal Data for various purposes subject to applicable laws and any applicable collective bargaining agreements. Personal Data we collect includes:

- Personal telephone number(s) and email addresses;
- Date and place of birth, age
- Nationality, gender
- Salary and benefits
- Identification numbers
- Private Bank Account
- Emergency contact information
- Job application letters and resume
- Health data such as severe disabilities, certificates of incapacity for work, etc.
- Issues reported through our so-called Ethics Hotline, a whistleblowing hotline for reports of unethical or illegal behavior

In addition to the examples listed above, Personal Data also includes general information such as name, middle name, surname, home address any other information disclosed in the course of an employee's application for employment that can be used to identify the individual.

Your Personal Data obtained by James Hardie will come primarily from yourself and from your managers or the Human Resources department. You will usually provide or have provided this information directly to your local Human Resources department.

Where permitted by applicable law in the specific case, we may also obtain some personal data from third parties, for example, references from a previous employer, or certain personal Data needed from tax authorities or benefit providers, or issues reported by other persons through our Ethics Hotline. Where this is the case, we will take reasonable steps to ensure that such third parties have represented to us that they have the right to disclose your Personal Data to us and upon request we will disclose the sources to you.

When we ask you for your Personal Data we will let you know whether it is mandatory that you provide the respective data and why. Failure to provide any mandatory Personal Data may mean that we cannot carry out certain Human Resources processes. As an example, if you do not provide us with information proving that you are eligible for certain benefits, we might not be able to grant these benefits to you.

Apart from Personal Data relating to yourself, you may also provide us with Personal Data of other natural persons, notably your dependents and other family members, for purposes of your Human Resource administration and management, including the administration of benefits and to contact your next-of-kin in an emergency. Before you provide such third party Personal Data to us you must first inform these third parties (or their legal representatives if they are minors) of any such data which you intend to provide and of the processing to be carried out by us and/or our affiliates and subcontractors for the purposes detailed below in the section headed "Why do we collect your Personal Data".

WHY DO WE COLLECT YOUR PERSONAL DATA?

We may collect and process your Personal Data for the following purposes, subject to applicable laws and any applicable collective bargaining agreements:

- Providing and administering remuneration, benefits and incentive schemes and providing relevant information to payroll;
- Recruitment, training, development, promotion, career and succession planning;
- Appropriate vetting for recruitment and team allocation including, where relevant and appropriate credit checks, right to work verification, identity fraud checks, relevant employment history and professional qualifications;
- Allocating and managing duties and responsibilities and the business activities to which they relate;
- To report and carry out work force analysis and for global enterprise head count reporting as well as consultations or negotiations with representatives of the workforce;
- Conducting surveys for benchmarking and identifying improved ways of working employee relations and engagement at work (these will often be anonymous but may include data such as age to support analysis of results);
- Managing and operating conduct, performance, capability, absence and grievance related reviews, allegations, complaints, investigations and processes and other informal and formal HR processes and making related management decisions;
- Managing reports of improper conduct on the basis of the James Hardie Ethics Hotline Policy to help ensure compliance with all applicable laws and regulations, promote the sound business practices embodied in Company policies and help avoid ethical misconduct and violations of the laws.
- Identifying and communicating effectively with staff;
- Operating email, IT systems, Internet, intranet and social media. We carry out monitoring of these systems (where permitted by applicable law respectively in the respective case) to protect and maintain the systems, to ensure compliance with company policies and to carry out internal investigations in compliance with applicable law;
- Processing information about absence or medical information regarding physical or mental health or conditions in order to assess eligibility for incapacity or permanent disability related remuneration or benefits, determine fitness for work, facilitate a return to work, adjustments or modifications to duties or the workplace. Management decisions regarding employment or engagement or continued employment or redeployment or termination and conduct related management processes;

- For planning, managing and carrying out restructuring or redundancies or other change programs including appropriate consultation, selection, alternative employment searches and related management decisions;
- Complying with applicable laws and regulation (for example maternity or parental leave legislation, working time and health and safety legislation, taxation rules, employee consultation requirements, other employment laws and regulations to which we are subject in the conduct of our business);
- Monitoring programs to ensure equality of opportunity and diversity with regard to personal characteristics protected under local anti-discrimination laws;
- Planning, due diligence and implementation in relation to a commercial transaction involving James Hardie that impacts your relationship with James Hardie (for example mergers and acquisitions or a transfer of your employment under automatic transfer rules);
- For business operational and reporting documentation such as the preparation of annual reports or tenders for work or client team records including the use of your personal photo (where permitted by applicable law respectively in the respective case, for example based on your consent);
- In order to operate the relationship with third party customer and suppliers including the disclosure of relevant vetting information in line with the appropriate requirements of regulated customers to those customers, professional contact or professional CV details or your personal photo for identification to clients or disclosure of information to data processors for the provision of services to James Hardie;
- Where relevant for publishing appropriate internal or external communications or publicity material including via social media, provided that privacy rights are preserved;
- To support HR administration and management and to operate the contract of employment or engagement;
- To centralize HR administration and management processing operations in an efficient manner for the benefit of our staff and to change access permissions;
- To provide support and maintenance for the IT systems;
- To enforce our legal rights and obligations, and for any purposes in connection with any legal claims made by, against or otherwise involving you;
- To comply with lawful requests by public authorities (including without limitation to meet national security or law enforcement requirements), discovery requests, or where otherwise required or permitted by applicable laws, court orders, government regulations, or regulatory authorities (including without limitation data protection, tax and employment), whether within or outside your country;
- To organize business trips and process travel bookings;
- For expense reimbursement purposes;
- For educational (training) purposes;
- To enable us to notify a family member in case of an emergency;
- Other purposes permitted by applicable privacy and data protection legislation including legitimate interests pursued by James Hardie and its affiliates where this is not overridden by the interests or fundamental rights and freedoms of staff.

This list is non-exhaustive. We have recorded a complete list of all the types Personal Data that we collect and process together with the purpose for the processing and we will make this list

available to you upon your request. Additional information regarding specific processing of Personal Data may be notified to you by your local Human Resources department.

LEGAL BASES FOR PROCESSING

As a general rule, James Hardie only collects and processes your Personal Data if there is a lawful justification to do so. We generally process your Personal Data as necessary under one or more of the following bases:

- Necessity for the performance of a contract to which you are party or in order to take steps at your request prior entering into a contract;
- Necessity for compliance with a legal obligation to which James Hardie is subject;
- Necessity in order to protect your vital interests or the vital interests of another natural person;
- For James Hardies' respective third parties' (in particular James Hardie affiliated companies) legitimate interests being those purposes described in the section above headed "Why do we collect your Personal Data";
- Occasionally your consent to the processing of your personal data where required and a legitimate legal basis under applicable laws.

In circumstances where the Personal Data that we collect about you is held by a third party, we will ensure you received prior notice of the collection and the source before we seek out this information from such sources (such permission may be given directly by you, or implied from your actions). Where permitted or required by applicable law or regulatory requirements, we may collect information about you without your knowledge or consent.

Processing of Special Categories of Personal Data

"Special Categories of Personal Data" include information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership, data concerning health or a person's sex life or sexual orientation, genetic data as well as biometric data for the purpose of uniquely identifying a natural person.

From time-to-time you may provide us with information which constitutes Special Categories of Personal Data or information from which Special Categories of Personal Data may be deduced.

As a general rule we will only process such data if you have expressly consented.
Employees who are employed in Switzerland should also note that the provisions regarding sensitive personal data under the Swiss Federal Act on Data Protection (FADP) apply.

You may withdraw your consent to the processing of Special Categories of Personal Data at any time by contacting your local Human Resource team, the Privacy and Data Protection Office or the local Data Protection Officer. Where you have withdrawn consent but James Hardie retains the Personal Data we will only continue to process that Special Categories of Personal Data where necessary for those purposes where we have another appropriate legal basis

(typically because processing is necessary in order to exercise specific rights or to comply with legal obligations derived from labour law, social security and social protection law). However, withdrawal of your consent may mean that we cannot (for example) administer certain benefits or provide support to you above and beyond our legal obligations.

Employees who are employed in France should also note that they may send specific instructions to James Hardie instructing on how James Hardie may continue to use personal data they withhold about those employees after their death regarding, in particular, the storage, erasure or disclosure of his/her personal data ("post mortem" right to privacy).

Where we are processing Special Categories of Personal Data and we do not have your explicit consent, we will only process that data where necessary:

- For the purposes of carrying out our/your obligations or to exercise our/your specific rights under employment, social security or social protection law (including employer whistleblowing laws);
- In exceptional emergency situations to protect your or another natural person's vital interests and you are physically or legally not capable at the time of giving consent (for example in a medical emergency);
- For reasons of substantial public interest, but only on the basis of EU or national laws (for example, preventing or detecting unlawful acts or complying with regulatory requirements relating to unlawful acts and dishonesty); or
- For the establishment, exercise or defence of legal claims.

Sensitive information may be processed in the following situations:

- Documentation such as work permits, details of residency and proof of citizenship will be processed to assess and review eligibility to work for James Hardie in the jurisdiction in which you work;
- Health and medical information may be used to comply with employment, health and safety or social security laws; for example, to provide statutory incapacity or maternity benefits, avoid breaching legal duties to you, to ensure fair and lawful management of your employment, avoid unlawful termination of your employment, to make reasonable adjustments and avoid unlawful discrimination or dealing with complaints arising in this regard;
- Your disability status may be used for the collection of statistical data subject to applicable laws, or where required to record such characteristics to comply with equality and diversity requirements of applicable laws;
- Trade Union membership may be recorded to ensure that you receive the specific rights that you are entitled to owing to any Trade Union membership, as required to enable us to meet our obligations under applicable employment law or if you have asked us to make payments directly to a Trade Union.

Processing of Personal Data Relating to Criminal Convictions and Offences

Personal Data relating to criminal convictions and offences will only be processed where authorized by applicable law. For example:

- A criminal record check may be carried out on recruitment or transfer where authorised by applicable laws;
- An allegation of a criminal offence or conviction arising during your relationship with James Hardie may be processed where required or authorised e.g. where we have a legal or regulatory requirement to report an offence or laws authorise James Hardie to process information about the offence for the purpose of making decisions regarding your relationship with James Hardie.

WHO HAS ACCESS TO YOUR PERSONAL DATA?

We may share your Personal Data with other members within the James Hardie group on a need-to-know basis including with:

- Local, regional and global Human Resource managers and Human Resource team members;
- Local, regional and executive management responsible for managing or making decisions in connection with your relationship with James Hardie or when involved in an Human Resource process concerning your relationship with James Hardie;
- Local, regional and global legal counsel and compliance officers and members of the Privacy and Data Protection Office;
- System administrators;
- Where necessary for the performance of specific tasks or system maintenance by staff in James Hardie teams such as the finance, global sales, marketing and IT department, global supply chain management and the global IT support team;.
- Certain basic Personal Data, such as your name, location, job title, contact information and any published skills and experience profile may also be accessible to other employees.

Your Personal Data may also be accessed by third parties with whom we work and who require such information for organizational, security and business purposes and to assist us with establishing and managing our employment relationship with you. This includes, for example, third parties that manage our payroll, provide information and data processing or storage services, or provide travel services.

From time to time, we may utilize the services of third parties (including other members of the James Hardie group) in our business and these members may also receive Personal Data collected by those third parties in the course of the performance of their services for us or otherwise. Where this is the case, we will take reasonable steps to ensure that such third parties have represented to us that they have the right to disclose your Personal Data to us.

In the context of the James Hardie Ethics Hotline, we have contracted with Navex Global Inc., a global company with its headquarters in Oregon, United States of America (hereinafter “Navex”)

to confidentially receive reports submitted via the Ethics Hotline. Many corporations utilize Navex as a confidential, external provider to oversee and administer their ethics hotlines. Reports submitted from the EU, UK and Switzerland will be received in the EU, and data relating to those reports will be hosted in the EU. The Head of Legal Europe will remove any Personal Data from the reports prior to sending them to the Ethics Hotline Principals.

Personal Data stored in our IT systems may also be shared with certain interconnecting systems such as, if applicable in your region, Concur, SAP, Success Factors and local payroll systems. Personal Data contained in such systems may be accessible by providers of those systems, their affiliates and their sub-contractors. To the extent that these systems have not yet been introduced and for introduction the involvement and approval of works councils is required, we will of course follow due process.

We may share Personal Data with members within the James Hardie group and third parties both in and outside of your home jurisdiction, and as result, your Personal Data may, for example, **but only if permitted by law**, be collected, used, processed, stored or disclosed in the United States of America.

Personal Data is only transferred by us to another country, including within the James Hardie group, if this is required or permitted under applicable privacy legislation, and in particular only in as far an adequate level of data protection of your Personal Data and rights are assured in the recipient country, according to the standards as set out by the European Commission or, where applicable, national governments.

When we share Personal Data with such members within the James Hardie group or third parties we typically require that they only use or disclose such Personal Data in a manner consistent with applicable European privacy standards.

In addition, Personal Data may be disclosed or transferred to another party (including to another member of the James Hardie group outside of your home jurisdiction) in the event of an (anticipated) change in ownership of, or a grant of a security interest in, all or a part of James Hardie through, for example, an asset or share sale, or some other form of business combination, merger or joint venture, provided that such party is bound by appropriate agreements or obligations and required to use or disclose your Personal Data in a manner consistent with the use and disclosure provisions of applicable European privacy standards. Further, your Personal Data may be disclosed:

- As permitted or required by applicable law or regulatory requirements. In such a case, we will endeavour to disclose only that Personal Data required under the circumstances;
- To comply with valid legal processes such as subpoenas or court orders;
- As part of James Hardie's regular reporting activities to other members of the James Hardie group (including outside of your home jurisdiction);
- To protect the rights and property of James Hardie;
- During emergency situations or where necessary to protect the safety of a person or group of persons;

- Where the Personal Data is publicly available;
- Where processing of employees personal data is regulated by collective agreements or
- With your consent where such consent is required by law.

Your data may be shared with the following third parties: tax authorities, James Hardies' insurers, bankers, IT administrators, lawyers, auditors, payroll providers, consultants and other professional advisors, but again only if we are permitted to do so by law. James Hardie expects such third parties to process any data disclosed to them in accordance with applicable law, including with respect to data confidentiality and security.

Where these third parties act as a "Data Processor" they carry out their tasks on our behalf and upon our instructions for the above-mentioned purposes. In this case your Personal Data will only be disclosed to these parties to the extent necessary to provide the required services and James Hardie will use all reasonable endeavours to have a data processing agreement in place covering the lawful and secure processing of Personal Data.

Sometimes we may share Personal Data with authorities in order to comply with a legal obligation to which we are subject. This is for example the case in the framework of imminent or pending legal proceedings or a statutory audit of our financial records.

TRANSFERRING PERSONAL DATA TO AND FROM YOUR LOCATION

To the extent permitted under applicable privacy legislation, Personal Data (including special categories of Personal Data) we collect from you may be processed and transferred outside of your home jurisdiction to, where applicable, for example, the United States or countries in Europe. Personal Data may also be transferred to third parties, as set out above, who may have systems or suppliers located outside your location. As a result, your Personal Data may be transferred to countries whose data protection laws may be different than the laws you are accustomed to and which laws may even be less stringent than the laws in your national jurisdiction.

James Hardie will ensure that appropriate and suitable safeguards are in place to protect your Personal Data and that transfer of your Personal Data is in compliance with applicable data protection laws. Where required by applicable data protection laws, James Hardie ensures that Data Processors and Data Controllers, which can include third parties and other members of the James Hardie group, sign standard contractual clauses ensure that your Personal Data is adequately protected in accordance with European standards. These standard contractual clauses are available on request. Also, where required to meet the standards of EU or UK privacy law, we will agree on supplementary measures with the respective Data Processor or Data Controller, as necessary.

Right to access, correct and delete your Personal Data and further data subject's rights

The European Union's General Data Protection Regulation and other countries' privacy laws provide certain rights for data subjects. James Hardie chooses to give all its employees, regardless of location, equal rights as described below.

Right of access and right to rectification: You have a right to request access to any of your Personal Data that James Hardie may hold, and to request correction of any inaccurate data relating to you. James Hardie aims to ensure the accuracy of all Personal Data. You also have a responsibility to notify James Hardie or any changes in personal circumstances (for example, change of address, salary account etc.) so that we can ensure that your data is up-to-date.

Right to erasure: Provided the legal requirements are fulfilled, you may request deletion of your data. This does not apply to Personal Data which is subject to a statutory retention period or which are necessary for the establishment, exercise or defence of legal claims. Insofar as access to such data is not necessary, however, its processing is restricted (see the following).

Right to lodge a complaint: You have a right to lodge a complaint with the appropriate data protection authority, in particular in the country off your residence, place of work or place of the alleged infringement if you consider that the processing of your Personal Data has, does or will infringe applicable law.

Right to restriction of processing: You have the right to restrict our processing of your Personal Data in certain circumstances.

Data portability: Where we are relying upon your consent or the fact that the processing is necessary for the performance of a contract to which you are party as the legal basis for processing, and that Personal Data is processed by automatic means, you have a right to receive all Personal Data which you have provided to James Hardie in a structured, commonly used and machine readable format, and also to require us to transmit it to another controller where this is technically feasible.

Right to object to processing justified on legitimate interest grounds: Where we are relying upon legitimate interest to process data, then you have the right to object to such processing on grounds relating to your particular situation, and we must stop such processing unless we can either demonstrate compelling legitimate grounds for the processing that override your interests, rights and freedoms or where we need to process the data for the establishment, exercise or defence of legal claims. Normally, where we rely upon legitimate interest as a basis for processing we believe that we can demonstrate such compelling legitimate grounds, but we will consider each case on an individual basis.

Right to withdraw consent: Where we are relying upon your consent to process data, you have the right to withdraw such consent at any time. You can do this by contacting your local Human resources team. Your withdrawal will not affect the lawfulness of processing based on your consent before its withdrawal.

Security of your information

To help protect the privacy of data and personally identifiable information, we maintain physical, technical and administrative safeguards. We update and test our security technology on an ongoing basis. We try to restrict access to your Personal Data to those employees who need to know that information, for example to provide benefits or services to you. In addition, we train our

employees about the importance of confidentiality and maintaining the privacy and security of your information.

Data storage and retention

Your Personal Data is stored on James Hardies' local servers and on the servers of the cloud-based services James Hardie engages. These cloud-based servers are typically located in the United States or in countries in the European Union. We try to encrypt your Personal Data where possible. Please contact the Privacy and Data Protection Office or where applicable the local Data Protection Officer for more information on data storage and retention.

How long do we keep your data?

Except as otherwise permitted or required by applicable law or regulatory requirements, James Hardie endeavours to retain your Personal Data only for as long as it is necessary to fulfil the purposes for which the Personal Data was collected (including, for the purpose of meeting any legal, accounting or other reporting requirements or obligations). This will usually be the period of your employment contract with us plus the length of any applicable statutory limitation period following your departure although some data, such as pension information, may need to be kept for longer. We may, instead of destroying or erasing your Personal Data, make it anonymous such that it cannot be associated with or tracked back to you. We may keep some specific types of data, for example, tax records, for different periods of time, as required by applicable law. However, some Personal Data may be retained for varying time periods in order to comply with legal and regulatory obligations. Further details can be found in the applicable document retention policy.

Additional Data Protection Notices

We may undertake certain processing of Personal Data which are subject to additional Data Protection Notices and we shall bring these to your attention where they apply.

Changes and updates to the Data Protection Notices

As our organization changes from time to time, this Data Protection Notice is expected to change as well. We reserve the right to amend this Data Protection Notices and you will be informed of these amendments or made aware that we have updated this Data Protection Notice and where to access the changed Notice on the appropriate platform so that you know which information we process and how we use this information. We may e-mail periodic reminders of our Data Protection Notice and will e-mail James Hardie employees of material changes thereto. The provisions contained herein supersede all previous notices or statements regarding our privacy practices.

Questions, concerns or complaints

Please contact James Hardie's Privacy and Data Protection Office or (for Germany) the Data Protection Officer:

Privacy and Data Protection Office	Data Protection Officer Germany
General	Germany (only)
Attn: Privacy and Data Protection Office Bennigsen-Platz 1 40474 Düsseldorf Germany Dpo@jameshardie.com	Attn: Data Protection Officer Bennigsen-Platz 1 40474 Düsseldorf Germany datenschutz-fermacell@jameshardie.com

Final Statement

This Data Protection Notice supersedes all previous statements or provisions made regarding data protection. The local language version shall prevail.