

Employee Code of Conduct

This Employee Manual & Code of Conduct, and the expected behaviours that are set out below, extends to all employees of Gordon McKay (**the Company** or **Gordon McKay**). While it does not form part of your contractual terms of employment, a failure to comply with any of the obligations may result in disciplinary action up to and including summary termination of your employment in cases of serious non-compliance.

1. Appearance/Dress Code

1.1. Clothing

It is expected that employees begin the workday with their work clothing in a clean, serviceable condition. Sun protection will be provided in the form of sunscreen. The wearing of shorts, T-Shirts and singlets (or less coverage) is not acceptable during working hours when on company business.

Office workers are expected to wear clean and tidy professional business attire.

1.2. Personal Appearance

It is expected that all employees present for work with a “clean” and professional image at all times.

All long hair must be properly contained in a suitable restraining device.

2. Personal Conduct

All employees are expected to demonstrate integrity, honesty and trust at all times at work, whenever representing the Company as well as outside of ordinary working hours. All employees are also expected to treat customers, fellow employees, contractors and members of the public with the utmost respect and courtesy at all times. The Company will not tolerate conduct which includes (but is not limited to):

- using objectionable, obscene or foul language or gestures towards employees, contractors or customers;
- “initiation” or “hazing” practices;
- horseplay;
- bullying;
- violence or threats of violence;
- stealing or other kinds of fraudulent or dishonest behaviour;
- offensive comments in relation to race, religion, gender, marital status, industrial activity, lawful sexual activity, political leanings or previous employment;
- the display of photographic material of a pornographic nature;
- unwanted sexual advances, lewd or suggestive remarks, or persistent unwanted attempts to initiate extra-curricular social activity;
- inappropriate use of Company information, systems or assets; or
- being found guilty of a serious criminal offence (in the reasonable opinion of the Company) or an offence that may cause reputational or commercial damage to the Company or prevent the employee from carrying out his or her duties.

A failure to meet or observe the personal conduct standards required by the Company may result in disciplinary action up to, and including, termination of employment.

3. Smoking

Employees are strictly prohibited from smoking:

- Outside of designated / approved smoking areas on all work sites;
- in or near company vehicles; and
- any other location directed by management of the Company

Employee Code of Conduct

4. Certificates of Compliance

All certificates must be correctly completed, dated and copies provided to the client at the earliest possible opportunity.

The supervisor must be notified in all instances where certificates cannot be lodged immediately upon completion of client work.

Certificates must be lodged by the employee with copies then provided to the client and employer in accordance with System Procedure 19 Conducting Routine Service Work and System Procedure 16 Project Planning and Management.

5. Health Monitoring

The Company has obligations in respect of employee and contractor health and safety. Prior to commencing work, employees and contractors must inform Gordon McKay of any pre-existing health or medical conditions that may be affected by the work that they are to perform. Should you require a job description or wish to confidentially discuss pre-existing injuries, you should contact your supervisor.

Section 41(2) of the *Workplace Injury Rehabilitation and Compensation Act 2013* will apply to any failure by you to make disclosure of such medical conditions, or making a false or misleading disclosure to the Company in relation to these matters prior to the commencement of work, which may result in you being precluded from access to worker's compensation in accordance with section 41(2) of the *Workplace Injury Rehabilitation and Compensation Act 2013*.

The company will also ensure your health is regularly monitored and you may be required by the Company to undertake:

- Medical examinations before employment and on an 'as required' basis.
- Medical examinations usually involving a general check-up, lung function (spirometry) and possibly a chest x-ray.
- Undertake hearing tests (audiometry)
- Random Drug and alcohol testing

These examinations and tests will be conducted at the Company's expense.

6. Medication

If you take medication please check with your health practitioner to establish if the use of the medicine will impact on work performance, especially if driving Company vehicles or operating machinery, or undertaking high risk activities forms part of your duties. You are required to obtain and provide to the Company advice in writing from your health practitioner that sets out any limitations or restrictions that may apply to your ability to carry out your duties while taking over the counter medication.

7. Personal Details

The Company needs to keep employee personal information up to date.

If any changes occur to the following, the Department Manager or HR Department needs to be notified as soon as possible;

- address;
- phone number;
- emergency contact details;
- bank details nominated for deposit of EFT wages;
- licence cancellations/suspensions;
- medical conditions that could possibly impair your ability to perform your duties in a safe manner.
- additional licenses and training courses completed; or
- your criminal record (including if you have been charged with any criminal offence).

Employee Code of Conduct

8. Protection of Personal Information

This section applies where an employee deals with personal information. Personal information means information or an opinion (whether true or not and whether or not in material form) about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion. The employee must:

- not use or disclose personal information obtained during the course of performing work for the company unless it is for company purposes;
- immediately notify the Company if you become aware of a breach, possible breach or unauthorised use or disclosure of personal information
- comply with any directions, guidelines, determinations or recommendations arising in relation to handling personal information while working for Gordon McKay; and
- ensure that any assistant/subcontractor of the Company who is required to deal with personal information is made aware of the obligations of the confidentiality conditions of Gordon McKay.

9. Confidentiality

You must not use, disclose or disseminate any Company confidential information acquired as a direct or indirect result of your employment with the Company at any time to any person, without the specific written authority of the Company or otherwise for carrying out your authorised duties. Confidential information must not be used for the personal benefit of the Employee.

For the purposes of this provision, 'confidential information' shall include, but is not limited to:

- (a) information relating to customers and suppliers of the Company;
- (b) financial information of the Company;
- (c) the Company's pricing information, including computations, algorithms, profit margins and internal estimating programs;
- (d) any information which relates to the commercial activities of the Company, including business plans, policies, procedures, price lists and information, sales plans, lists of suppliers or licensing partners, customer lists, product information, intellectual property, business notes or memoranda or professional development or education material provided to you by the Company or paid for by the Company or strategies of the Company;
- (e) any business negotiations between the Company and any third party;
- (f) information designated as confidential by the Company; and
- (g) information which is not in the public domain, or is only in the public domain due to a breach of this clause by the Company.

Your obligations relating to confidential information continue to apply, notwithstanding the expiry or termination of your employment

10. Requirements Before Termination of Employment

Before leaving the Company, all stock, plant, tools and keys to Company buildings, vehicles and plant boxes must be returned to your manager.

Any fines received by the Company for which, you are responsible, will remain your responsibility to pay after you have left the Company.

You must advise your manager of any computer file passwords that may have been generated over the term of employment.

All outstanding job sheets, purchase orders and time sheets must be completed and submitted prior to your last day of work with the Company.

Confirmation will be obtained from your manager regarding your compliance with these obligations, before your final pay is released.

11. Late Attendance or Absenteeism

Late attendances and absenteeism must be advised to your immediate supervisor or manager at the earliest possible opportunity. Repeated late attendance, without reasonable excuse, may result in disciplinary action being taken.

Employee Code of Conduct

12. Theft

All Company employees are responsible for secure and proper storing of vehicles, cables, tools, materials and other forms of Company equipment.

Failure to properly secure Company equipment or materials may lead to disciplinary action being taken, which may include dismissal in serious cases of non-compliance.

All thefts of Company equipment must be reported immediately to your manager who will then take the necessary action which may involve making a report to the police and you may be required to assist with their enquiries.

13. Drivers Licence

It is your responsibility to possess a valid driver's licence at all times and, depending on your duties, may be a fundamental term of your engagement.

You must advise your manager if at any time you do not possess a valid driver's licence.

Any employee who drives a Company vehicle whilst not possessing an appropriate driver's licence will be deemed guilty of serious misconduct and may have his or her employment terminated without notice.

14. Jury Duty

You must immediately notify and supply supporting documentation to your manager if you are required to perform jury duty.

The Company will continue to pay your ordinary wages for the duration of the jury duty however proof of attendance must be produced.

If payment is received by you for undertaking jury duty, you are required to reimburse the Company the amount that you received for jury duty.

There will be no additional payment or compensation by the Company where jury duty occurs over a weekend or on any other day where you would not have normally been required to attend work for the Company.

15. Telephone Policy

15.1. Overview

Telephone communication, whether by fixed or mobile telephone, is an integral part of daily business. Gordon McKay aims to use telephones in a manner which assists employees to effectively and flexibly perform their responsibilities, ensures enhanced client service, while maintaining efficiency, safety and fair and responsible use.

The use of telephones must be as cost effective as possible. The following principles must be observed when using Company telephones:

- The number of calls made should be limited to those necessary for effective business.
- Private use of telephones should be kept to a minimum.
- The user is responsible for any and all activities associated with the phone issued to them.

15.2. Use of Mobile Phone While Driving

In order to ensure your safety and the safety of other road users, mobile phones should never be used while driving a motor vehicle unless using an approved hands free car kit. Even then, mobile phone users must take care not to become distracted while using the hands-free phone. A failure to observe this provision is also an offence under road safety legislation.

It is recommended that hands free mobile phones should not be used when operating a vehicle; that the user should safely park the vehicle before taking or making a call. Responsibility in this matter rests with the user.

Employee Code of Conduct

15.3. Lost, Stolen or Mislaced Mobile Phones

Due to the high incidence of mobile phone theft and misuse after loss, a mobile phone service must be cancelled immediately if lost or stolen. The theft or loss should be reported to the nearest police station and your supervisor to have the phone barred.

To reduce the risk of theft, employees must ensure mobile phones are not visible in a vehicle when it is unattended.

15.4. Mobile Phone Use

The Company monitors the monthly usage of mobile phones. Any excessive private use, in the reasonable opinion of the Company, must be reimbursed by the employee.

If employment is terminated or the employee leaves the Company, the mobile phone must be returned to the Company prior to the employee's final day of work.

As work sites have various policies relating to the use of mobile phones all Gordon McKay employees must consult direct with the client or their supervisors upon restrictions placed on the use of mobile phones. Unless prior arrangements have been made (on a case by case basis) with the client or their supervisor, personal mobile phones may only be accessed during meal breaks and before and after work hours in the designated areas.

Be aware, recent court precedents involving material that can be considered offensive may be in breach of discrimination and equal opportunity legislation and may also be regarded as a criminal offence.

Where Company issued mobile phone users receive text messages/electronic messages from an external source and the user decided that the material may breach this policy, you are required to delete the material immediately and where possible discourage the originator from resending similar material.

Use of a phone to access internet material which is considered offensive is also prohibited and is subject to the Company's IT policy.

Company staff have access to direct dial telephones throughout the offices and specific sites when established. Private reverse charge calls are not to be received on the company phones. Private local calls are to be kept to a minimum. STD calls are to be kept to a minimum and the cost of private calls may have to be repaid to the Company. International calls are not to be made without the permission of your direct supervisor.

16. Time Sheets

Time sheets must be completed on a daily basis so that accurate records can be kept of the hours and jobs that have been conducted. The time sheet must contain the date, job number, job name, start and finish times and hours worked for each job.

The time sheet(s) must be received at the office by the close of business every Friday, unless working on the weekend.

Time sheets which arrive late may not be processed for that week's pay.

17. Wages

Employees' wages are calculated and paid weekly.

Wages are paid by electronic transfer into the employees' bank account.

Payment of wages will not be made in cash.

Employee Code of Conduct

18. I.T. Policy

18.1. General

- 18.1.1. The Company has software and systems in place that monitor and record all internet usage. Our security systems are capable of recording (for each and every user) each World Wide Web site visit and each email message into and out of our internal networks, and we reserve the right to do so at any time. No employee should have any expectation of privacy as to his or her internet usage. Our managers will review internet activity and analyse usage patterns and they may choose to publicise this data to assure that company internet resources are devoted to maintaining the highest levels of productivity.
- 18.1.2. The Company reserves the right to inspect any and all files stored in private areas of our network in order to assure compliance with policy.
- 18.1.3. The display of any kind of sexually explicit document or multimedia on any Company system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, stored, distributed, edited or recorded using the Company's network or computing resources.
- 18.1.4. The Company uses independently supplied software and data to identify inappropriate or sexually explicit internet sites. We may block access from within our networks to all such sites that we know of. If you find yourself accidentally accessing a site that contains sexually explicit or offensive material, you must leave that site immediately, notwithstanding that the site was still accessible.
- 18.1.5. Employees must not install any software or hardware to any Company computer or network without first receiving express permission from management. Any software or files downloaded via the internet into the Company network become the property of the Company. Any such files or software may be used only in ways that are consistent with their licenses or copyrights.
- 18.1.6. No employee may use Company facilities to download or distribute pirated software or data.
- 18.1.7. No employee may use the Company's internet facilities to propagate any virus, worm, Trojan horse or trap-door program code.
- 18.1.8. No employee may use the Company's internet facilities to disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of another user.
- 18.1.9. Each employee using the internet facilities of the Company shall identify himself or herself honestly, accurately and completely (including one's Company affiliation and function where requested), when setting up accounts on outside computer systems.
- 18.1.10. Employees are reminded that it is prohibited to reveal confidential Company information, customer data, trade secrets and any other material covered by existing Company secrecy or confidentiality policies and procedures on the internet. Employees releasing such confidential information – whether or not the release is inadvertent – may be subject to disciplinary action up to and including termination of employment.
- 18.1.11. Because a wide variety of materials may be considered offensive by colleagues, customers or suppliers, it is a violation of Company policy to store, view, print or redistribute any document or graphic file that is not directly related to the user's job or the Company's business activities.
- 18.1.12. Employees with internet access may not upload any software licensed to the Company or date owned or licensed by the Company without the express authorisation of the manager responsible for the software or data.

Employee Code of Conduct

18.2. Email

- 18.2.1. Email is used as a business communication tool and employees are required to use this tool in a responsible, effective and lawful manner. It is important that employees are aware of the legal risks of email.
- 18.2.2. By following the guidelines in this policy, employees can minimise the legal risks involved in the use of email. If any employee disregards the rules set out in this email policy that employee will be held responsible and may be subject to disciplinary action.
- 18.2.3. Employees should be aware that email can be subject to court orders for production as evidence in legal proceedings.

The following rules are imposed by law and are required to be strictly adhered to.

It is prohibited to:

- (a) Send or forward emails containing potentially defamatory, discriminatory, bullying, harassing, offensive, racist or obscene remarks or content. If you receive an email of this nature you must promptly delete the email or notify your direct supervisor.
 - (b) Forge or attempt to forge email messages.
 - (c) Disguise or attempt to disguise your identity when sending email.
 - (d) Send email messages using another person's email particulars or account.
 - (e) Copy a message or attachment belonging to another user without permission of the originator.
 - (f) Send an email containing the Company's confidential or privileged information
- 18.2.4. The Company's email system is supplied, and intended to be used primarily as a business tool. The sending of personal emails, chain letters, junk mail, jokes, sexually explicit material or games or program files is not permitted.

18.3. Technical

- 18.3.1. User IDs and passwords help maintain individual accountability for internet resource usage. Any employee who obtains a password or ID for an internet resource from the Company must keep that password confidential. Company policy prohibits the sharing of user IDs or passwords obtained for access to internet sites.
- 18.3.2. The use of a password to gain access to the computer system, or any part of the computer system, does not provide employees with an expectation of privacy in the computer system in any document accessed.

18.4. Security

- 18.4.1. The Company has installed an internet firewall to assure the safety and security of the Company's networks. Any employee who attempts to disable, defeat or circumvent any Company security facility will be subject to immediate dismissal.
- 18.4.2. Only those internet services and functions with documented business purposes for this Company will be enabled at the internet firewall

Employee Code of Conduct

19. Social Media

- 19.1. The Company appreciates the growing development and use of social media throughout society and how it creates an online forum to create, share and consume content. The Company also acknowledges that social media can share a connection with the workplace, either intentionally or unintentionally, which now creates new responsibilities for the Company and its employees. This policy applies to employees who use the following:
- multimedia and social networking websites such as Facebook, My Space, Yahoo Groups, YouTube, LinkedIn, Twitter and other similar sites;
 - blogs, both the Company approved and personal; and
 - Wikis such as Wikipedia and any other site where text can be posted.
- 19.2. The Company acknowledges that interest in the above sites also extends to corporations which are recognising that social media offers new opportunities to engage with their customers and community organisations.
- 19.3. While the Company embraces the development and use of social media as a new tool for corporate and community engagement, it also requires its employees to consider and familiarise themselves about the potential crossover between personal use of social media and how this may impact on the Company and their employment with the Company.
- 19.4. Employees should be aware that a violation of this policy may result in disciplinary action including a verbal or written warning or, in serious cases, termination of employment. The Company may seek to recover any costs incurred by it as a result of a breach of this policy by an employee. The employee may also be personally liable if the law is broken in respect of any matters set out in this policy.
- 19.5. Everything written on the internet can be traced back to its author through a range of methods. It is also common for social media content to be reposted in other areas of the internet and other non-digital forums, therefore once content is posted by an author, it can be difficult for it to be removed. Once posted the author has no control about the number of times the content can be reposted or by whom it is reposted. Employees are required to take these factors into account when using any social media or publishing content on the internet, having regard to how such content may be stored or used and its potential to impact on the interests of the Company.
- 19.6. There is not always a clear distinction between an employee's conduct in his or her personal life and work life. Even though content may be published by an employee outside of work hours and not relate directly to work does not mean there will not be a connection with, or impact to, the employee's employment with the Company. Communication between employees outside of work hours through social media sites or reference being made to other employees or the Company outside of work hours may be treated as an employment issue for which an employee, if found in breach of this policy, may be disciplined, or in serious cases, have his or her employment terminated.
- 19.7. Employees must not publish any confidential or proprietary information of the Company or its customers, nor disclose other employees' personal information.
- 19.8. Employees must not publish any content which could cause damage to the reputation of the Company, its directors or employees.
- 19.9. Employees must not post or link any materials that are defamatory, harassing, discriminatory, bullying or indecent. Employees should be respectful of the opinion of others and not post any material that is obscene, defamatory, threatening, harassing, discriminatory or hateful to anyone else. Employees' obligations under the *Equal Opportunity Act 2010 (Vic)* and the *Racial and Religious Tolerance Act 2001* apply equally online as in all other areas.
- 19.10. Employees are encouraged to pause before publishing content on the internet and to consider the possible implications of the content being posted. Content published by employees is treated as their own personal comments and not those reflected of Gordon McKay, therefore it is the employees' responsibility to ensure that such content is appropriate in the circumstances.

Employee Code of Conduct

20. Conflict of Interest

- 20.1. Except with the prior written consent of the Company, you must not for the duration of your employment with the Company compete, be employed by, involved with or have an interest in any other business which conflicts with the best interests of the Company, the requirements of your position or your ability to perform your duties.
- 20.2. You must avoid any conflict of interest which may arise between you and the Company and at the earliest opportunity declare all facts to the Company which may give rise to a conflict.
- 20.3. You must also avoid accepting payment or other benefits from any other person as an inducement or reward for any act or forbearance in connection with any matter done on behalf of the Company.

21. Issue Resolution Process

Refer to Form 041 the Issue Resolution Flowchart

22. Misconduct

- 22.1. It is Company policy that employees wilfully engaging in acts that create or increase safety risks to either themselves or others will have their engagement terminated summarily.

The following list (which is not exhaustive) contains examples of offences which constitute serious misconduct which may give rise to summary dismissal:

- Unauthorised possession of property, money, confidential information or intellectual property belonging to or under the control of the Company.
- Possession or use of the property of other employees without the owner's permission.
- Refusal to undertake the duties of the employee's position or to carry out any proper and lawful instruction delivered by person acting with the authority of the Company.
- Walking off the job without authority.
- Physical violence or the incitement of any such physical violence against any persons on the premises or at a work place where Company employees work.
- Racial, sexual or other improper harassment of an employee, contractor, customer or member of the public.
- Being at work intoxicated (whether drugs or alcohol) as to prevent or impede the proper performance of duties (whether of the employee himself/herself or of any other employee). Refer to separate procedures.
- Being on licensed premises without permission during work hours.
- Deliberate use of an unauthorised password in order to enter or attempt to enter, a computer known to contain information to which the employee is not entitled to have access.
- Failure to observe safety procedures or working in an unsafe manner, or failing to make proper use of safety equipment where such equipment is installed or supplied.
- Falsification of any records or any action which could result in a payment to which an employee is not entitled.
- Abuse of special leave such as sick leave or bereavement leave.
- Operating a vehicle without a current drivers' licence or the appropriate class of licence for that vehicle.
- Any wilful act causing or likely to cause injury or danger to life.
- Unauthorised disclosure of confidential information.

Employee Code of Conduct

22.2. Other Misconduct

The manager will record all misconduct and warnings given and a copy will be issued to the employee.

The following are acts or omissions (not exhaustive) which may, after the appropriate warnings lead to dismissal.

- Persistent failure to achieve any performance standards set or incompetence in the performance of an employee's duties short of gross incompetence.
- The use of abusive, obscene or threatening language to another person in the workplace.
- Disruption of the workplace by acts of undesirable behaviour or horseplay.
- Unauthorised absence from duty.
- Smoking in no-smoking areas.
- Any act which is likely to diminish the good reputation of Gordon McKay in the community.
- Without good reason, failing to notify the supervisor as close as possible to the normal commencing time that the employee will be late or unable to commence work for that day.
- Failure to report any work accident that requires medical treatment, within 24 hours.
- Failure to notify Gordon McKay within two working days of being disqualified from driving.
- Defacing Gordon McKay property.
- Failure to maintain or take due care of Gordon McKay property (including vehicles).
- Unreasonably frequent and persistent lateness or absence.
- Any act or omission which, while not being serious misconduct, has a significant effect on an employee's ability to carry out the duties of the employee's position.
- Any other act or omission which, while not specifically covered by the foregoing classes of misconduct, is of a similar nature.