HUMAN RESOURCES POLICY

Table of Contents

1. INTRODUCTION

1.1 Purpose

The purpose of this Human Resources Policy is to set out how DirectMoney Ltd and its various wholly owned subsidiary companies (hereinafter referred to as “DM” or “Company”) manages its employees.

1.2 AIM OF THE POLICY:

This policy aims to:

- promote and develop good employment practices;
- attract and retain a skilled workforce that is committed to DM’s vision, mission and values;
- develop a culture of openness, honesty, trust, respect, teamwork and a pro-active mindset;
- promote equal opportunity;
- encourage professional and self-development through learning, education and training opportunities;
- continuously improve the performance of employees and to take appropriate steps to improve poor performance;
- ensure adequate human resources are in place as required under the Company’s Australian Credit Licence and Australian Financial Services Licence;
- put in place core controls to reduce and/or mitigate key human resources risks; and
- ensure compliance with any industry related or employment legislation, such as privacy, NCCP, anti-discrimination, Fair Work Act, Worker’s Compensation or WH&S

1.3 Application of Policy

This policy applies to all employees of DM.

1.4 Identifiable Risks and Controls

This Human Resource Policy puts in place core controls to reduce and/or mitigate the following key human resource risks:

- Breach of applicable employment legislation or employment contract;
- Recruitment of unsuitable employees;
- Employee skills and performance levels, including a high level of customer complaints;
- Employee satisfaction/morale levels;
- Abuse of employees’ benefits or incorrect salary payments;
- Employee fraud or theft;
- Breach or non-compliance with any industry related or employment legislation, such as privacy, NCCP, anti-discrimination, Fair Work Act, Worker’s Compensation or WH&S;
- Loss of productivity;
- Unacceptable employee turnover levels.

Some of the other key controls (all of which will be further discussed in this policy) are:

- Roles and responsibilities clearly defined by personal objective setting (when appropriate) and a performance review process;
- Conditions of employment communicated and understood;
- Board and Chief Executive Officer communication;
- Individual employment contracts in place and accepted (when appropriate);
- Recruitment processes and succession planning;
- Induction and training of new staff;
- Performance management systems in place;
- Work Health and Safety standards clearly defined;

- Regulatory compliance;
- Internal control systems in place.

2. VISION, MISSION, VALUES

2.1 Vision

Our vision is to become Australia's most respected and innovative Marketplace Lender accounting for a growing share of the $100 billion unsecured consumer credit market and with $500 million of personal loan assets under management.

2.2 Mission

We connect borrowers and investors by leveraging technology to offer competitively priced loans and provide attractive loan investment products for retail and institutional investors

2.3 Values

Our core values are:

TRUST

We gain the trust of investors, borrowers and stakeholders by maintaining high ethical standards, transparency and robust business practices.

INNOVATION

We believe that innovation coupled with the flexibility and discipline to make timely changes to our business processes will continue to be a potent source of competitive advantage.

TEAMWORK

We strive to be the best we can be as individuals, yet recognize we can only succeed through working as a team and showing respect and support for all team members.

3. RECRUITMENT

3.1 Recruitment Strategy

Recruitment policies and practices have a significant impact on culture, climate, member relationships, fraud and ultimately DM's profit and performance.

Fundamental to DM's success is the need to recruit and retain the number and quality of employees required to achieve our objectives and to provide a competent and flexible workforce who will deliver in a rapidly changing environment. Attracting the right people into the organisation, the first time, will improve attrition and retention levels of the people who epitomise the values and aims of the Company.

3.2 Recruitment Policies

To ensure the success of DM's recruitment strategies, the recruitment of all new employees to the Company will be subject to the following policies:

- Approval to fill vacancies, change existing roles or create new roles rests solely with the Chief Executive Officer and other key nominated Managers when authority has been delegated.
- The Chief Executive Officer will be involved in all job grading, salary, redeployment or consultation considerations.
- All potential candidates will be subject to an interview, usually by at least two people, one of whom will be the potential candidates immediate superior.
- References which are work-related with a preference from a previous supervisor must be independently checked.
- All potential staff will be subject to a National Police check prior to appointment.
- The final selection and appointment process rests with the Chief Executive Officer or nominated Managers when specifically delegated.

3.3 Recruitment Advertising

DM will adopt the following policies in respect of all advertising:

- Role specification to be completed and with agreed salary (grade) by the Chief Executive Officer prior to any advertisement being placed.
- The advertisements must accurately describe the key elements of the role, will not be misleading and emphasise that DM is an equal opportunity employer.

3.4 Induction

On commencement of employment, all staff will be provided with a job description, a copy of this policy document, and will be provided with induction training and an overview of DM's operations and aims by a Manager.

3.5 Probationary Period

Unless otherwise stated in your offer of employment, all new employees are subject to a minimum probation period of six (6) months. The probationary period gives DM the opportunity to assess the employee's performance on the job.

Probationary periods may also be implemented due to misconduct or poor job performance.

4. PERFORMANCE MANAGEMENT AND TERMINATION

4.1 Performance Evaluations

The performance of all employees directly impacts on the performance of teams, business units, and the overall performance of DM. This policy has been developed to ensure an employee's performance is managed effectively.

DM supports and fosters a performance review process in order to promote frank, honest and open communication between employees and the Chief Executive Officer at a formal level. Performance reviews assist member service levels, goal setting, identifying training requirements and risks to the business.

The Performance Management System consists of:

- role specifications clearly defining individual responsibilities, activities and key performance indicators; and
- annual performance reviews;

The Performance Management System ensures:

- performance evaluations provide a formal opportunity for two-way feedback and are not used as a means of disciplining an employee.
- reviews are conducted privately and do not involve a third party unless mutually agreed upon.
- discussions undertaking the evaluation process are confidential between DM and the employee concerned.

4.2 Counselling and Disciplining

DM aims, at all times, to provide an opportunity for employees to respond accordingly if their performance or conduct is being questioned. This policy has been developed to ensure procedural fairness and to create an environment that is conducive to the resolution of performance and/or conduct issues.

The following policy and process is required to be observed by all employees:

- Where possible Chief Executive Officer (in respect of Managers) or Managers (for all other staff) should aim to provide coaching to pre-empt counselling or disciplining.
- The counselling/disciplinary process may include a combination of one or both of the following steps:
  - **Informal Discussion** — The Chief Executive Officer or a Manager discusses the performance with the employee and may make a diary note to the discussion for reference. The employee is advised of the required performance and the consequences of failing to reach the advised standard.
  - **Formal Counselling** — The Chief Executive Officer discusses the performance with the employee and a written record of the meeting is kept. The employee is given a letter outlining the expected performance standard and the consequences of failing to reach that standard. This is considered a formal warning.
- All employees must be made aware of the counselling and disciplining procedure at the beginning of each meeting relating to performance or conduct.
- A written record must be made by the Chief Executive Officer when counselling occurs, and a copy placed in the employee's personnel file.
- At all counselling sessions it must be made clear to the employee what the consequences of poor performance, behaviour or conduct will be and whether termination is a possible outcome.

- The Chief Executive Officer should ensure someone senior to the employee or another Manager is present when conducting a formal disciplinary meeting.
- The employee should be offered an opportunity to respond to any file note if a disciplinary notification is issued.
- The employee must be given every opportunity to respond to any issues raised.
- All disciplinary matters are confidential and are not to be discussed with anyone apart from a Chief Executive Officer or those directly involved in the meeting.
- Misconduct offences that may warrant immediate dismissal include the following, but are not limited to these specific examples:
  - abusive language or behaviour towards employees or customers;
  - any action or behaviour, on or off duty, likely to damage DM's reputation and standing;
  - accessing/downloading or on-forwarding pornographic or offensive material;
  - using the Internet for purposes which are strictly excluded in Board Polices;
  - consuming illegal drugs or using illegal substances, or being under the influence of these while at work;
  - fraud of any kind, including falsifying timesheets or the manipulation of any records or company data;
  - possessing weapons in the workplace;
  - refusal to carry out a reasonable instruction from an immediate supervisor or Chief Executive Officer;
  - any form of harassment, coercion or discrimination;
  - theft, violence, rudeness and abusive or threatening behaviour.

4.3 Grievance Handling

DM takes pride in promoting a fair, open and honest work environment that encourages employees to discuss any concerns or grievances they may have without fear of reprisal.

Grievances are to be resolved quickly and efficiently as failure to do so may result in a negative impact on employees and the Company. For the Chief Executive Officer or managers involved in handling any personal grievance, the following policy applies:

- A grievance is a clear statement by an employee of a work related problem, concern or complaint, including persons or equipment involved.
- If an employee has a concern about the way they are being treated in the work place or the way, in which a situation directly affecting them has been handled, they have a right to raise their concern. The employee must provide the Chief Executive Officer or manager with an opportunity to resolve the issue in the first instance.
- The Company must ensure that all employees are aware of and are able to access the grievance procedure.
- An employee who reports a grievance will be provided with information on the course of action (including options) that may be taken.
- All grievance matters are confidential and should only be discussed with the relevant parties to the grievance.

4.4 Terminations (Voluntary)

The Company acknowledges the importance of processing terminations in a timely and efficient manner. It also values the feedback obtained from exit interviews conducted with terminating employees. This assists with the continual refinement of systems and business practices.

The following policies apply in the voluntary termination of employees:

- When an employee terminates employment voluntarily, they are required to notify the Company (usually a manager) in writing.
- The Chief Executive Officer is responsible for ensuring the employee receives their final pay and any outstanding monies owed.
- If the employee does not provide sufficient notice, in accordance with their employment contract, they may have money deducted from their final pay in lieu of the period of notice not given.
- An employee may finish earlier than their required notice period provided there is mutual consent between the employee and the Company.

4.5 Terminations (Involuntary)

DM reserves the right to dismiss, without notice, any employees found to have acted in a manner that constitutes gross misconduct as defined in the Code of Conduct (as set out in Annexure 1 of this Policy).

The following policies apply in managing all involuntary terminations:

- The Chief Executive Officer with the required authority must be notified and approve the dismissal of any employee.
- Before terminating an employee, the Chief Executive Officer will ensure that the termination is not harsh, unjust or unreasonable and that DM's performance counselling and discipline procedures have been observed.
- In the normal course, the Chief Executive Officer or a Manager should be present at any dismissal interview.

5. CONDITIONS OF EMPLOYMENT

5.1 Code of Conduct

All employees of DM must adhere to DM's Corporate Code of Conduct – the minimum standard of workplace behaviour expected from employees of DM

The Corporate Code of Conduct is set out in **Schedule 1** of this Policy.

5.2 Privacy of Information

DM is governed by many different governmental Acts and it is important that it complies with all requirements of each Act.

The Privacy Act is a Federal Commonwealth Government Act that aims to protect each individual and ensures an individual's rights to privacy and the privacy of their personal information. All employees must abide by the relevant "Privacy Legislation" and DM's Privacy Policy.

DM collects and holds personal information in relation to customers and employees.

Personal information means any information which identifies an individual or from which an individual's identity can be reasonably ascertained. Name, address, telephone numbers and employment details are examples of personal information.

Sensitive information means information or an opinion about an individual's racial or ethnic origin, political views, religious beliefs or affiliations, union memberships, criminal history, sexual preferences or health information.

DM values employees' privacy and will protect and maintain the privacy, accuracy and security of their personal information to the full extent provided by the law.

It is a requirement that all employees fully understand and observe their personal obligations under the Privacy Act in all dealings with DM customers and guests, suppliers and other employees.

Access to an employee's personal file will be limited to the employee, the Chief Executive Officer/Managers, or other employees who have a justifiable need to know. An employee has the right to access his/her file and has the right of reply to information contained in their personal file.

5.3 Affirmative Action and Equal Opportunity

DM has a strong commitment to the practical application of equal opportunity within all facets of its operations. This includes ensuring that employee management practices are conducted in a fair and equitable manner at all times. Every individual will have an equal opportunity to apply for a position within the organisation subject to having the necessary skills, knowledge, qualifications and experience.

The following policies apply:

- DM will not tolerate illegal discrimination against any employee.
- The merit principle will form the basis for all decision-making in the areas of recruitment, remuneration, promotions and professional development.
- Decisions will only be based on the relevant experience, potential and the aptitude of applicants.
- Equal opportunities will be provided to all employees in terms of training, development, formal feedback, remuneration, and benefits.
- Any reports of illegal discrimination will be treated promptly and investigated thoroughly, maintaining confidentiality as required.
- Any employee who is guilty of having illegally discriminated against another employee or potential employee will face disciplinary action.

5.4 Harassment

DM is committed to a policy which endeavours to protect employees at all levels from harassment in the workplace. Harassment can occur through various means including sexual harassment, workplace bullying and discrimination. The following is DM's standard policy on harassment:

- Harassment in the workplace will not be tolerated under any circumstances. Harassment is any form of:
  - intimidation,
  - abuse,
  - offensive behaviour,
  - humiliation of a sexual or non-sexual nature, or
  - workplace bullying.
- Every employee that commences employment with DM will be provided with awareness and training on the "Harassment" policy.
- An employee may be uncomfortable with telling a colleague or Chief Executive Officer that behaviour is uninvited and inappropriate towards them. In such cases, witnesses may note the employee's body language and report the behaviour as harassment.
- Complaints of harassment will be treated seriously and confidentially.

Sexual Harassment

Sexual harassment is any unwelcomed or uninvited behaviour of a sexual nature. Examples may include, but are not limited to:

- unwelcome touching;
- personal remarks;
- displaying sexual materials;
- telling jokes of a sexual nature;
- written or e-mailed material of a sexual or personal nature;
- inappropriate gestures;
- inappropriate leering at a person or body part;
- making promises in return for sexual favours or making threats if sexual favours are withheld;
- persistent questions or insinuations about a person's private life;
- stalking.

Sexual harassment may occur as a single incident or as an ongoing pattern of behaviour directed toward one or more people.

If a person witnesses behaviour that makes them feel humiliated or offended, it may amount to sexual harassment of that person, even though the offending behaviour is not directed towards that person.

DM will at all times act to ensure employees are treated with fairness and all matters of sexual harassment will be thoroughly investigated to ensure natural justice is provided to all parties.

Workplace Bullying

Workplace bullying includes, but is not limited to:

- shouting at or intimidating an employee;
- using obscene or abusive language;
- pushing or using physical force;

- threatening body language;
- threats of dismissal as opposed to a formal warning of dismissal;
- unreasonable requests;
- singling out an individual;
- humiliating an individual;
- constant criticism;
- gossip.

Workplace bullying is usually identified when there is an ongoing pattern of behaviour directed toward one or more people.

5.5 Redundancy, Redeployment and Retrenchment

DM is committed to a policy which attempts to minimise the retrenchment of employees wherever possible. Redundancy, redeployment and retrenchment policy and procedures are governed by the applicable legislation, awards and individual employment contracts. The following policies apply:

- All retrenchments must be approved by the Board.
- All redeployment options will be considered.

When positions are made redundant, employees must be treated with dignity and fairness in supporting their efforts to find alternative employment either within or outside the Company.

5.6 Work Health and Safety

DM is required to comply with the work health and safety legislation which in NSW is the Work Health and Safety Act 2011 (NSW) following agreement in July 2008 to adopt new national model Work Health and Safety (WH&S) laws in most states and territories.

The workplace safety and health of all people employed in DM and those visiting DM are considered to be of the utmost importance. Resources will be made available to comply with all the relevant WH&S Acts and regulations to ensure that the workplace is safe and without risk to health.

The Chief Executive Officer has approved a separate policy which sets out the guidelines and legislated requirements to ensure full compliance with WH&S regulations. This is set out in Section 8 of this policy. All staff are provided with a copy of this policy at the time of their commencement of employment with the Company.

Breach of the policy is considered serious misconduct and can result in disciplinary action including termination of employment.

5.7 Smoke Free Work Environment

There is strong scientific evidence that passive smoking is hazardous to health. In accordance with its legal obligations to protect the health and safety of those who work at or visit DM, the Company has developed the following smoke-free workplace policy:

- **Smoking Bans** - Smoking is prohibited within the confines of all DM offices.
- **Assistance to Quit Smoking** - Professional help, including quit smoking advice and information, is available for employees who may require assistance to adapt to the policy.
- **Smoking Breaks** - In harmony with a smoke-free work environment, the Chief Executive Officer and supervisors will not encourage or approve breaks for employees to smoke during work hours.
- **Adherence to Policy** - Employee observance of this policy is a condition of employment. Any breach of this policy will incur normal disciplinary procedures. It should be noted that employees who fail to follow this policy can be disciplined for non-compliance, and if non-compliance continues, their employment may be terminated.

5.8 Abandonment of Employment

DM will ensure that a procedure is applied and followed in incidents where an employee is suspected of abandoning the workplace without notice or reason.

This policy will ensure that the correct steps are followed and an employee suspected of abandoning the workplace is provided with a fair opportunity to inform the employer as to why they are not at work before the employer terminates their employment. The following policy applies:

- Abandonment of employment occurs where an employee does not attend their workplace for a period of three (3) days or more without notifying their employer to provide a valid explanation as to why they are absent.
- The employee's supervisor must make all reasonable effort to contact the employee when the employee has failed to show for work without providing a reason for being absent.

5.9 Whistleblower Protection Program

DM is committed to a Whistleblower Protection Program to ensure there is an unhindered obligation to effective reporting of corrupt and illegal practices that are contrary to the Code of Conduct and the Human Resources Policy, by people at all levels.

Reportable conduct by a person or persons connected with the Company, in the view of the whistleblower acting in good faith, is:

- dishonest or unethical conduct;
- fraudulent or illegal conduct;
- corrupt or other serious improper conduct;
- an unsafe work practice;
- a breach of legislation;
- any other conduct which may cause financial or non-financial loss to DM.

6. SALARIES & WAGES, LEAVE, EXPENSE CLAIMS

6.1 Salaries and Wages

DM recognises that an effective remuneration system is essential to the success of its operations and to mitigate the risk of losing key employees. It is committed to a policy of individually negotiated remuneration contracts, using established practices, for all employees.

Remuneration of all contracted personnel will be reviewed at least annually by the Chief Executive Officer as applicable.

Salaries are paid directly into your nominated bank account monthly, via electronic transfer. A payslip will be delivered to you within two business days of your pay day.

6.2 Hours of Work

The nature of DM's business involves a five day week operation. Company hours are variable dependent on business requirements and are necessarily flexible to ensure return for the costs involved.

Hours of work for all permanent or permanent part-time staff are specified in individual employment contracts or per agreement between supervisor and employee. Casual staff hours are subject to variation based on the needs of the business.

6.3 Leave

6.3.1 Annual/Holiday Leave

Annual Leave (also known as holiday leave) is granted to employees based on the provisions of their entitlements under relevant legislation including the Fair Work Act 2009 governing their employment conditions which is currently 20 days per annum (based on an employee's ordinary hours of work). Part-time employees are entitled to a proportionate amount of annual leave. DM will respond to leave requests in a flexible manner, but may restrict certain types of leave depending on business requirements.

The following policies apply with respect to annual leave arrangements:

- If you wish to apply for leave you are required to complete a DM Leave Application Form and submit this to your Manager for approval at least two weeks prior to the requested first day of leave. The responsible manager must then forward approved leave form to the Office Manager for record keeping purposes. Applications will not be granted unless an employee has accrued, via annual entitlements, sufficient leave time.
- You are encouraged to take leave in week or fortnight blocks wherever possible.
- You may be requested to take leave if provided with one month's notice in writing.
- No more than six (6) weeks of annual leave can be accumulated without approval from the Chief Executive Officer.
- If *Leave-without-Pay* is granted in conjunction with annual leave, your payroll entitlements are frozen for the duration of the unpaid leave.

A sample of DM's Leave Application form can be found in Schedule 2 of this Policy. The actual form can be found in DM's Google Drive > Company Info > Forms > Leave Forms.

6.3.2 Personal Leave (Sick/Carer's)

Personal leave is granted to employees based on their employment contract and in accordance with their entitlements under relevant legislation and the Fair Work Act 2009 which is currently up to a maximum of 5 days per annum. The following policies apply in respect of sick leave and carer's leave arrangements:

Sick Leave

- Sick leave is cumulative from year to year.
- You must notify your relevant Manager and Office Manager via email, telephone or text message as early as possible when absence is expected.
- Upon your return, you are required to complete a DM Leave Application Form and submit this to your Manager with any applicable documents (see below) for approval. The responsible manager must then forward approved leave form to the Office Manager for record keeping purposes.
- For two or more consecutive days' absence, a medical certificate is required to be attached to your leave form.
- If you are absent on either side of a public holiday, a medical certificate is also required.
- DM may request for you to provide a medical certificate for any absence claimed as sick leave if patterns are suspect or excessive leave has been taken historically.
- If you require time off for a future medical procedure, you will be required to provide a medical certificate for that leave period.
- A medical certificate must be in the form of a Doctor's Medical Certificate, recognised by the Australian Medical Association.
- You may request to use any annual leave accrued to ensure you are paid for any time taken for sick leave should your sick leave accrual be insufficient to cover your period of absence.

Carer's Leave

- Carer's leave is also available to employees and forms part of the personal leave entitlement as defined by relevant legislation and the Fair Work Act 2009.
- Carer's leave may be granted if an employee's spouse, de facto spouse, child, parent, or sibling is sick.
- You must notify your relevant Manager and Office Manager via email, telephone or text message as early as possible when absence is expected.
- Upon your return, you are required to complete a DM Leave Application Form and submit this to your Manager with any applicable documents (see below) for approval. The responsible manager must then forward approved leave form to the Office Manager for record keeping purposes.
- DM may require you to establish that your family member was sick and needed care. A medical certificate is sufficient in these cases.

A sample of DM's Leave Application form can be found in Schedule 2 of this Policy. The actual form can be found in DM's Google Drive > Company Info > Forms > Leave Forms.

6.3.3 Long Service Leave

Long Service Leave will accrue in terms of the Long Service Leave Act 1955 after working for an unbroken period of ten years with an employer. The leave will be paid at the salary rate that is applicable when the leave is taken.

To qualify there needs to be continuous service with an employer, even if the workers' duties or position is changed during that time.

6.3.4 Compassionate Leave

DM's employees, full or permanent part-time, are entitled to a maximum of two days leave as defined in the Fair Work Act 2009 without loss of pay on each occasion when a member of an employee's immediate family or household:

- Dies;
- Suffers a life-threatening illness or injury.

Immediate family is an employee's:

- Spouse or former spouse;
- De factor partner or former de facto partner;
- Child;
- Parent;
- Grandparent;
- Grandchild;
- Sibling; or a
- Child, parent, grandparent, grandchild or sibling of the employee's spouse or de facto partner.

This definition includes step-relations (e.g. step-parents and step-children) as well as adoptive relations.

Employees will be able to take compassionate leave for other relatives (e.g. cousins, aunts and uncles) if they are a member of the employee's household, or if the employer agrees to this.

If taking compassionate leave, you must notify your relevant Manager and/or Office Manager via email, telephone or text message as early as possible.

Upon your return, you are required to complete a DM Leave Application Form and submit this to your Manager for approval. The responsible manager must then forward approved leave form to the Office Manager for record keeping purposes.

DM may request evidence about the reason for compassionate leave (e.g. death or funeral notice or statutory declaration).

6.4 Expense Claims

DM employees who incur expenses arising out of DM's business are entitled to a reimbursement of these expenses subject to approval from the employee's Manager prior to incurring the expense.

An expense claim form (see Schedule 3 for sample) is required to be completed with receipts for the expenses attached to the form. The completed form with receipts are to be submitted to their relevant Manager for approval. Once approved, the relevant Manager must submit this to the Office Manager for processing.

6.5 Internal Controls

The Chief Executive Officer will ensure that acceptable controls are in place to mitigate the risk of fraud or malpractice within the salary payment system by developing appropriate procedures covering salary rate changes and variations, payroll, leave, employee data and information, and employee actual monthly and quarterly cost comparisons.

The Office Manager will provide a quarterly reconciliation of all outstanding annual leave for all permanent and contracted staff, reporting movements from the previous quarter end and including leave accrued and leave taken.

The controls will be regularly tested on an annual basis by external auditors.

7. COMPUTER USE, INTERNET AND EMAIL

7.1 IT and Computer Policy

Overview

DM's systems provide a valuable tool for conducting business in the Company. The following rules have been established to ensure the proper use of equipment, network and electronic communications, as well as safeguard all information that is transmitted or received on it.

The Company requires policies and rules on protecting our corporate information by governing the use of DM's IT systems. This document serves as the policy and reference point for all staff of DM on the internal information security policy.

All messages, documents and information conveyed by or contained within DM's electronic resources – including correspondence, attachments etc – are the property of DM.

A copy of this policy will be issued to each staff member. Routine compliance audits may be conducted to ensure adherence to the policy and its guidelines. Whilst this policy covers the key IT policy requirements, if other serious offences or events occur that are not contained in this policy, disciplinary action will be taken at Board discretion.

Introduction

Computer information systems are an integral part of business and are costly. These policies and directives have been established in order to:

- Protect this investment.
- Safeguard the information contained within these systems.
- Reduce business and legal risk.
- Protect and maintain the good name of the Company.

Violations

Failure to observe these guidelines may result in disciplinary action by the Company depending upon the type and severity of the violation, whether it causes any liability or loss to the Company, and/or the presence of any repeated violation(s).

Statement of Responsibility

Security is everybody's responsibility and it is a requirement of employment with DM that all staff will adhere to and comply with this policy. The following sections list additional specific responsibilities for DM and its employees.

The Chief Information Officer (CIO) will ensure that all appropriate staff are aware of and comply with this policy and create appropriate performance standards, control practices, and procedures designed to provide reasonable assurance that all employees observe this policy.

Systems Access and Security

DM's websites are implemented using up-to-date best coding practices and regularly tested against numerous known online threats. Public access is made available to DM's public facing website, and the administration website is restricted to authorised accounts only. Each authorised person is issued a unique account that is assigned roles that restrict available operations, and a strict password policy is enforced.

DM's websites are constantly reviewed to ensure integrity, availability and security. DM's development team monitors internet threats and regularly test the service to ensure it remains secure.

Several third-party services are used by DM staff, each dictates their own security standards that are reviewed and approved by the CIO. The CIO appoints administrative staff to maintain access privileges to each system as required.

7.2 Access Codes and Passwords

Passwords should be protected at all times. Managers and employees are ultimately responsible for any information that is sent from their electronic communications. User ID and DM information that you are privy to is Confidential and it is therefore important that electronic communications and access privileges are safeguarded.

Any password lists maintained by any staff must be maintained in a password protected document. Hard copies of passwords must be stored in a secure location, such as a safe.

Frauds and Passwords

When an employee signs on to any DM computer or online service, they are adopting responsibility for transactions that occur under their name. This is particularly important relative to fraud and passwords. **Fraud** can take many forms, and technology has broadened this even further. Users must not:

- Impersonate another person (e.g. by using someone else's password or by using a computer signed on as someone else).
- Tamper with e-mail (e.g. amending a stored message; making an e-mail appear to be from someone else).

Passwords — Subject to the policy outlined above, Users are responsible for the use of their password(s) and must be careful to prevent misuse of access. The following procedures must be observed:

- Users should not tell their password(s) to anyone else nor should they allow anyone else to sign-on using their password. If an employee requires access to facilities that they do not have, they should speak to their manager.
- Should password(s) become known to others, change it (them) immediately.
- Avoid writing down passwords, unless they can be stored securely.
- Passwords should be changed regularly or immediately if there is any indication of possible system or password compromise. When choosing a new password avoid re-using one recently used.
- Users must log off or lock their computer when they are going to be away from it for any significant period of time, including lunchtime and leaving the office for the day.
- Any misuse of password should be reported to the Chief Executive Officer or Office Manager immediately.
- Users should change temporary passwords at the first log in.

7.3 Viruses and Causes

A virus is a self-reproducing program, maliciously hidden in another program, which can become active at any time.

If the program is downloaded or copied, the virus may spread and corrupt further disks and programs, which may lead to important information being destroyed, damage to systems or loss of systems access. Viruses can arrive via e-mail or can be downloaded from the internet and users should not open any unusual e-mails from an unrecognized source. Should an employee receive an unusual e-mail or from an unrecognized source, they must not open it and report it immediately to the Chief Information Officer.

To guard against viruses, users must:

- Store files on the hard drive which is constantly checked for viruses.
- Always save any file attachments received via email that are not shortcuts or links directly to the hard drive before viewing.
- Not run unauthorized copies of programs.
- Report any message about viruses that appear on their screen to the Chief Information Officer. Users must not use their PC for anything until they are satisfied that it is safe to do so.

Installation of software

No unauthorised employee should install any unauthorized or incompatible software onto a DM computer, or onto DM devices.

No DM employee should download or install any piece of software on to DM devices, for business purposes or otherwise, without prior consent from the Chief Information Officer. This includes downloading of software from internet sites, and installation of screensavers, games, or other peripheral programs.

Software installed on devices owned by employees is permitted, but may be reviewed by the Chief Information Officer or appointed staff at any time, and a request may be issued to either remove the software, or discontinue connections to DM services from the device.

Employee Responsibilities

These policy requirements apply to all employees:

1. Employees shall not knowingly introduce a computer virus into company computers.
2. Employees shall not load diskettes, removable drives or media of unknown origin.
3. Virus scanning software must not be interrupted, turned-off, removed or tampered with in any way.
4. Anyone who suspects that their workstation has been infected by a virus shall discontinue using the device to connect to DM services, and report the issue to the Chief Information Officer or Office Manager.

7.4 General Use and Ownership

DM's computer systems are solely designed to accommodate the business needs and activities of the Company. Therefore, users should avoid using the system for personal use or storage of personal information. Because of the need to protect and maintain DM's assets, management cannot guarantee the confidentiality of information stored on any network drive, PC hard drive or any other electronic storage facility that becomes connected with DM online or onsite services. Nor can DM guarantee that personal information will not be deleted or published without the individual's knowledge or consent.

Where users do make personal use of the system they should be aware that privacy of the data they create on corporate systems is not protected by law and the data is accessible to DM.

For security and network maintenance purposes, authorised individuals within DM (or any outsource partners) may monitor equipment, systems, e-mail activity and network traffic at any time.

The Company has the right to audit networks and systems on a periodic basis to ensure compliance with this policy. This monitoring can occur without your specific consent or knowledge at that time.

Acceptable Usage

All users must:

- keep passwords secure and must not share network user-IDs. Authorised users are responsible for the security of their passwords.
- ensure that all PCs, laptops, phones and tablets used to access DirectMoney information services are secured with a password-protected device lock feature, with the automatic activation feature set at 10 minutes or less of inactivity. Devices should be explicitly locked when left unattended.
- If a device has multiple users with different accounts, keep sensitive customer or business files stored on local devices to protected folders (eg. C:\Users\username).
- If a laptop, usb stick or other portable data storage device is to contain sensitive data and taken outside the office, then consider using encrypted folders.
- exercise special care to protect all data on portable computers because information contained on portable computers is especially vulnerable.

These policies must be followed on all devices used to connect to DM's onsite or online network services.

Unacceptable Usage

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by DM.
- Introduction of malicious programs into computing devices, networks or online services.
- Revealing your password or allowing use of your user-ID by others, including work colleagues. This includes family and other household members when work is being done at home.
- Using a DM computer to actively engage in procuring or transmitting material that is in violation of the *Code of Conduct*.
- Tampering with or disabling the automated malware detection systems in place on all devices.
- Any security breaches or disruptions of network communication. These types of breaches include:
  - accessing data of which the employee is not an intended recipient;
  - logging into a server or account that the employee is not authorised to access;
  - unauthorised use of any network sniffing, pinged floods, packet spoofing, denial of service, port scanning or similar utilities;
  - executing any form of network monitoring which will intercept data;
  - circumventing user authentication or security of any host, network or account.

  When accessing DM services from a device that is not owned and controlled by DM or a DM employee or contractor:

  - At no time should passwords be saved on the non-DM-related PC, nor should the password be given to a family member or friend.
  - At no time should you disclose any detail of DM's online services.

Employee Responsibilities

For on-site systems, the following directives should be followed by all employees:

1. USB thumb drives and portable storage devices should be stored out of sight when not in use. If they contain highly sensitive or confidential data, they must be locked away.
2. Portable storage devices and other data storage media should be kept away from environmental hazards such as heat, direct sunlight, and magnetic fields.
3. Environmental hazards to hardware such as food, smoke, liquids, high or low humidity, and extreme heat or cold should be avoided.
4. Employees shall not take shared portable equipment such as laptop computers out of the office without the informed consent of their department manager. Informed consent means that the manager knows what equipment is leaving, what data is on it, and for what purpose it will be used.
5. Mobile employees using portable equipment such as laptops or notebook computers out of the office must ensure these assets are properly secured and not left unattended or in plain view
6. Employees should exercise care to safeguard the valuable electronic equipment assigned to them.

Employees who neglect this duty may be accountable for any loss or damage that may result.

7.5 Internet Policy

This policy sets out guidelines for acceptable use of the Internet in the Company. The primary purpose for which access to the Internet is provided is to assist in carrying out any duties of employment or contract.

Employees (or delegated individuals) are not to use the Internet in such a way as to significantly interfere with the duties of their employment (or contract) or to expose DM to significant cost or risk of liability.

Internet - Acceptable Uses

The Internet may be used for —

- Work-related purposes.
- Sending and receiving personal e-mail messages, provided:
  - the volume is kept to a minimum and normal work duties are not impacted;
  - all email messages (and user group postings) have a disclaimer to the effect that the views of the sender may not represent those of DM.
- Sending and receiving e-mail attachments that are work related. Use extreme caution when opening e-mail attachments received from unknown senders; they may contain viruses or other malicious computer programs.
- Accessing the World Wide Web for personal purposes. This is discouraged and should be kept to a minimum.
- Streaming recreational audio services, so long as bandwidth consumption is kept within tolerable levels.

In all cases there should be only minimal personal use. Unnecessary usage could incur additional costs and may interfere with the employment duties of the employee. Users are responsible at all times to use the DM's computer resources in a professional, ethical and lawful manner.

The Internet can be utilised for the following type of activities as long as they do not conflict with policy guidelines:

- Conducting personal research;
- Surfing or browsing the Web.

Additionally, personal use of the Internet must not:

- Interfere with the work performance of the user or his/her colleagues;
- Have an undue impact on the operation of the DM's computer systems related to the download of information or introduction of viruses;
- Violate any provision of this policy.

Internet - Unacceptable Uses

Unless required for conducting work-related activities, Internet access must not be used for:

- sending personal advertisements and non-work related e-mails to distribution lists except in the course of an employee's duties.
- sending SPAM or unsolicited bulk e-mails, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material.
- disseminating any confidential information of DM, its customers, vendors, without proper authority to do so. Individuals must know what is and is not acceptable based on their position and function or the nature of their contract with the Company.
- any form of harassment, including abusive, hateful, degrading, demeaning, derogatory or defamatory materials, information or communication via e-mail through language, frequency, or size of messages.
- any illegal purpose.
- placing any business information on any publicly-accessible Internet locations without Board approval;
- participating in electronic discussion sites (i.e., chat rooms, bulletin boards) as a representative of DM;
- developing your own business-related Web site;
- accessing Web sites, computer systems and networks on the Internet for which you are not authorised;
- disseminating personal contact information of officers or employees of DM without their consent.
- unauthorised use, or forging, of e-mail header information or identification.
- accessing any gambling or related sites and/or participating in any form of gambling activities via the internet.
- accessing sites or downloading any material that may be regarded as pornographic, obscene, sexually explicit, indecent or otherwise offensive in nature or that would contravene the Code of Conduct.
- knowingly causing any other person to view content which contravenes acceptable business practice.

Users may not upload (i.e. transfer from DM computers or systems to the internet) any software licensed to DM or data owned or licensed by DM without explicit authorisation from the Chief Information Officer, Chief Executive Officer or the Board.

Users may not use Company facilities to download or distribute pirated or illegal or copy righted software/data, entertainment software, music or games.

Users may not use DM's Internet facilities to deliberately spread any virus, worm, Trojan horse, or trap-door program code.

Additional Prohibitions and Requirements for Internet Access

- Unauthorized access to remote Internet sites, application ports, mail designated ports, FTP, WWW or other internet services is strictly forbidden;
- The use or possession of password cracking programs or Internet security tools are strictly forbidden;
- Users must not attempt to circumvent established DM Internet security measures.
- Users must not delete internet activity or history records.

7.6 E-mail Usage Guidelines

Users should carefully consider the intended audience, tone, formality, and format for all e-mail messages.

Any message received which is intended for another person should be returned to the sender. All copies of the misdirected message should be deleted after it has been returned to the sender. An incorrectly addressed message should only be forwarded to the intended recipient if the identity of that recipient is known and certain.

Monitoring and Enforcement of Policy

All messages created, sent, or retrieved over the Internet are the property of the Company and may be regarded as public information. Computer surveillance is carried out on an ongoing basis. This surveillance may be continuous or intermittent. The Chief Information Officer or Chief Executive Officer may monitor records at any time.

All communications, including text and images, can be disclosed to law enforcement or other third parties without prior consent of the sender or the receiver. This means don't put anything into your e-mail messages that you wouldn't want to see on the front page of the newspaper or be required to explain in a court of law.

DM reserves the right and has the ability to monitor, access and review at any time, on a continuous or intermittent and ongoing basis computer surveillance on all internet usage, all messages, documents and information transmitted and received on DM's systems.

This computer surveillance may include the use of:

- Email messages (including personal emails) and other electronic messaging systems– including the content of every email message received, sent or stored on DM computers including laptops. This also includes emails deleted from the inbox.
- Internet use (including internet use for personal purposes) this includes internet tracking, that is every URL visited which is traceable including the time of access, the duration of access and any documents downloaded from a URL site.
- Other electronic files and documents (including personal documents) created, modified, sent, received or stored using any DM electronic resources.

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Downloads and Uploads

File downloads from the Internet are currently permitted as long as they relate to business needs, such as business content documents, white papers, product information, business brochures, system updates, etc. It must be stressed that downloading or installing of executable programs is not permitted.

If a program, utility, or executable file is required this must be requested from and/or authorised by the Chief Executive Officer. Installation of executable programs onto company assets without approved licensing or authorisation can jeopardise the security of the network and confidential data and this may result in disciplinary action.

This policy may be reviewed from time to time or on a case-by-case basis at the discretion of the Board and file download access can be restricted or revoked if found to be unproductive or unauthorised in nature.

Copyrights

Employees using the Internet are not permitted to copy, transfer, rename, add, or delete information or programs belonging to others unless given express permission to do so by the owner.

Failure to observe copyright or license agreements may result in disciplinary action by the company and/or legal action by the copyright owner.

Employee Responsibilities

An employee who uses the Internet or Internet e-mail shall:

1. Ensure that all communications are for professional reasons and that they do not interfere with his/her productivity.
2. Be responsible for the content of all text, audio, or images that are placed or sent over the Internet. All communications should have the employee's name attached.
3. Not transmit copyrighted materials without permission.
4. Know and abide by all applicable Company policies dealing with security and confidentiality of Company records.
5. Ensure applications designed to protect Company assets and data such as virus scans, security settings and firewalls are not adjusted, bypassed, turned off or removed from any computers or tampered with in any way that could expose confidential file(s) to the Internet.
6. Avoid transmission of non-public member information. If it is necessary to transmit non-public information, employees are required to take steps reasonably intended to ensure that information is delivered to the proper person who is authorised to receive such information for a legitimate use.

8. WORK HEALTH AND SAFETY

8.1 Legislative Requirements and Policy

DM is required to comply with the work health and safety legislation which in NSW is the Work Health and Safety Act 2011 (NSW) following agreement in July 2008 to adopt new national model Work Health and Safety (WH&S) laws in most states and territories.

In terms of the legislation, DM is defined as a PCBU (a "Person Conducting a Business or Undertaking") and the primary responsibility for work health and safety in the workplace lies with the PCBU rather than an employer alone.

DM, as a PCBU, has a primary duty of care to ensure, so far as reasonably practicable (see Section 8.2 below), that workers and all other persons (for example clients or people visiting our premises), are not exposed to health and safety risks arising from our business activities or undertakings. This duty covers both workers engaged, or caused to be engaged, by DM, and workers whose activities in carrying out their work are influenced and directed by DM.

DM has a duty of care that applies "*to the extent to which the person has the capacity to influence and control the matter*."

The workplace safety and health of all people employed in DM and those visiting the Company are considered to be of the utmost importance. Resources will be made available to comply with all the relevant WHS Acts and regulations to ensure that the workplace is safe and without risk to health.

8.2 Work Health and Safety Program

DM has a primary duty of care to ensure the health and safety of workers while they are at work and that for ensuring that work carried out does not carry risk to the health and safety of others. This means that DM is required by law to:

- Provide and maintain a safe work environment.
- Provide and maintain safe plant and structures.
- Provide and maintain safe systems of work.
- Ensure the safe use, handling and storage of plant, structures and substances.
- Provide adequate facilities (and ensure access is maintained).
- Provide instruction, training, information and supervision.
- Monitor the health of workers and conditions at the workplace.

DM must ensure, so far as is "reasonably practicable", that workers or other persons are not exposed to health and safety risks arising from its business or undertaking and takes into account and weighs up all relevant matters including:

- The likelihood of the hazard or risk concerned occurring.
- The degree of harm that might result from the hazard or risk.
- What the person concerned knows, or ought reasonably to know, about the hazard or risk, and ways of eliminating or minimising the risk.
- The availability and suitability of ways to eliminate or minimise the risk.
- After assessing the extent of the risk, and the available ways and the costs associated with eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.

In order to implement the general provisions of the legislation and DM's policy, a program of activities and procedures will be set up, continually updated and effectively carried out.

The program will relate to all aspects of WH&S including:

- Directors and officers will have an express duty to exercise due diligence to ensure that DM is complying with its WH&S obligations.
- DM will implement a risk management program through which it will take positive steps to identify workplace hazards, assess each hazard in terms of likelihood and potential consequence, and take action to either eliminate or reduce all hazards identified.
- WH&S training and education.
- Work design, workplace design and standard work methods and practice, including those associated with technological change.
- Safety rules.
- Emergency procedures and drills.
- Provision of WH&S equipment, services and facilities.
- Workplace inspections and evaluations.
- Reporting and recording of incidents, accidents, injuries and illnesses and provision of information to employees, contractors and sub-contractors.

Consultation with Staff

The law creates a positive obligation on DM, as far as is reasonably practicable, to consult with staff in relation to workplace safety matters. Consultation requires:

- Sharing of health and safety information.
- Providing workers with a reasonable opportunity to express their views, raise issues and contribute to the decision making process.
- Taking the views of workers into account and advising on the outcome in a timely manner.

There is an obligation to consult when:

- Identifying and assessing risks to health and safety, deciding ways to eliminate or minimise those risks and deciding on the adequacy of facilities for workers' welfare.
- Proposing changes that may affect the health and safety of workers.
- When deciding on procedures for consulting with workers, resolving WH&S issues, monitoring workers' health, or monitoring conditions at the workplace under the control of DM.
- Providing information or training for workers.

As a staff member you are in the best position to identify potential workplace hazards and to make recommendations with respect to the implementation of risk control measures. DM encourages the involvement of all staff in making ours a safe workplace. Your views are valued and will be taken into account.

DM has appointed a WH&S Officer to provide a clear communication channel for staff wishing to provide input or feedback with respect of our WH&S and Injury Management and Return to Work programs.

Health and Safety Committee

DM is not required by law to convene a formal Health and Safety Committee unless five workers request that such a committee be established. DM will not establish a committee unless requested to do so as our WH&S Officer has the necessary power to authorise action in response to the Board's decisions and requirements and any other matters to ensure the Company maintains full compliance.

Health and Safety Representative

Under the legislation, if one staff member asks for a Health and Safety Representative ("HSR") to be appointed, then DM is required to comply. The Act provides specific eligibility criteria, procedures for the election and training of the HSR. Roles and responsibilities are set out in Section 8.3 below.

8.3 Roles and Responsibilities

All Managers and individuals who perform work on behalf of DM have a part to play in ensuring we maintain a safe workplace. Specific roles and responsibilities are set out below.

Managers/Employers

All Managers and employers have an obligation to ensure the general health, safety and welfare at work of all employees as well as other workers (such as contractors) who may be present in DM's workplace.

Managers/Supervisors

The law extends workplace responsibility to managers and supervisors who are directly responsible for workplace safety within areas under their control. Management at all levels are required to contribute to the health and safety of all people in the workplace.

Each manager is required to ensure that this policy and the WHS program are effectively implemented in their areas of control, and to support supervisors and hold them accountable for their specific responsibilities.

Each first-line manager or supervisor is responsible, and will be held accountable, for taking all practical measures to ensure that the workplace under their control is safe and without risks to health, and that the behaviour of all persons in the workplace is safe and without risks to health.

More specifically:

- The supervisor will always be held accountable for detecting any unsafe or unhealthy conditions or behaviour.
- If the supervisor does not have the necessary authority to fix a problem, they will be held accountable for reporting the matter promptly together with any recommendations for remedial action to the Chief Executive Officer or a Manager who does have the necessary authority.
- The Chief Executive Officer or Manager who has the necessary authority will be held accountable for taking prompt remedial action to eliminate any unsafe or unhealthy conditions or behaviour.

Employees/Workers

As an employee (including the Chief Executive Officer, and all employees, managers and supervisors) you are required to comply with the WHS policy and programs to ensure your own health and safety and the health and safety of others in the workplace.

You must:

- Cooperate with DM in anything that you are required to do in order to ensure a safe workplace including:
    - Notifying your supervisor of actual and potential hazards
    - Wearing or using prescribed safety equipment
    - Carrying out work in a safe manner
    - Following health and safety instructions
    - Taking notice of signs
    - Participating in safety training.
- Take reasonable care for the health and safety of co-workers and ensure your actions do not put co-workers at risk;
- Work safely;
- Use and maintain any equipment properly;
- Ensure that your work area is free from hazards.

As a worker **you must not:**

- Intentionally or reckless interfere with or misuse anything provided in the interests of health, safety and welfare;
- Move or deface signs;
- Tamper with warning alarms;
- Play practical jokes that may put the health and safety of others at risk;
- Behave in a way that results in risk to others;
- Intentionally hinder or obstruct the giving or receiving of any form of aid when a person is injured at work.

Contractors and Sub-Contractors

All contractors and sub-contractors engaged to perform work on the DM's premises or locations are required, as part of their contract, to comply with DM's WH&S policies, procedures and programs and to observe directions on health and safety from designated officers of the organisation.

Failure to comply or observe a direction will be considered a breach of the contract and sufficient grounds for termination of the contract. Visitors who fail to follow directions should be asked to leave the premises.

Clients or Visitors

All clients and visitors to DM premises have a positive obligation to:

- Take reasonable care for their own safety.
- Take reasonable care to ensure their acts or omissions do not adversely affect the health and safety of other persons.
- Comply with any reasonable instructions from DM or its officers and staff.

The Role of the Health and Safety Representative

If elected under the legislation, the Health and Safety Representative has expanded powers to:

- Investigate complaints.
- Inspect the workplace.
- Attend interviews with the regulator or the PCBU.
- Issue provisional improvement notices (as defined by the Act).
- Issue directions to cease work.

The Role of the WHS Officer

The WHS Officer's general duties include:

- Monitoring changes in legislative requirements and ensuring DM is adhering to these requirements.
- Monitoring the effectiveness of DM's Workplace Safety Program with respect to their particular work group.

In respect of DM's WHS Program, the WHS Officer is responsible for reviewing measures taken to ensure the health, safety and welfare of all persons at their place of work. This includes:

- Facilitating the training of all staff and managers with respect to the operation of our WHS Program and our Injury Management and Return to Work Program.
- Investigating any matter that may be a risk to health and safety in the workplace and carrying out workplace inspections.
- Providing a clear **communication** line with employees with respect to WHS and Injury Management issues, including the management of the consultation process.
- Communicating with staff with respect to the **identification of workplace hazards.**
- **Assessing the risks** posed by the workplace hazards identified.

- Co-ordinating the implementation of appropriate risk treatments and controls.
- Investigating workplace injuries and taking appropriate steps to prevent/control such injuries in the future.
- Maintaining an “Incident Register” in terms of legislated requirements.
- Resolving any other WHS issues.

8.4 Training, Education and Supervision

DM is committed to **train, educate and supervise** staff in relation to workplace safety matters. At DM we meet this obligation in the following ways:

- **Training** — All new staff joining DM are required to undertake specific WH&S training. Staff must be provided with training on our WHS and Injury Management and Return to Work programs.
- **Specific Individual Training Requirements** — Where we identify that a worker, contractor or other visitor to the workplace may be exposed to specific hazards, further training will be undertaken.
- **High Visibility of Workplace Safety Programs and Policies** — All our programs and policies are published on our shared DM Google Drive and therefore readily accessible to all workers who may wish to review these documents.
- **Short Form Policy Statements and Signage** — DM has developed Short Form Policy Statements that are displayed prominently within the workplace together with signage designed to encourage the early identification or workplace hazards and reporting of workplace injuries. These statements are reviewed on a regular basis.
- **Ongoing Training and Education** — On a regular basis all staff are requested to consider the workplace hazards identified and the treatments and controls implemented, and to provide feedback to the WHS Officer as to the overall effectiveness of the programs.
- **Emergency Evacuation Procedures** — Ongoing education is provided for the emergency evacuation of DM’s premises in the event of a fire or other emergency.

The staff **consultation** and **training and education** procedures are designed to ensure that staff are aware of WHS issues and have a clear channel for communicating workplace hazards.

8.5 Identification of Workplace Hazards

DM has a positive obligation at law not only to identify hazards that could harm employees, contractors or other persons at the workplace but to **analyse** the level of risk posed by the hazard and to **treat** or **control** the hazards identified. To assist the **hazard identification** process DM has developed the following systems and procedures.

Hazard Register

Based upon hazards that would typically be expected to be present in a workplace such as ours and historical experience of workplace injuries, DM has developed a register of potential workplace hazards.

The **Hazard Register** provides a useful reference point for the continuing process of hazard identification within the workplace.

Monitoring Changes in the Workplace

It is the role of the WHS Officer to review changes in the workplace and to assess hazards that may emerge from these changes. Typically changes in the workplace occur when:

- We occupy new premises or extend our existing premises.
- New plant or equipment is introduced into the workplace.
- Hazardous substances are introduced into the workplace.
- New work practices are introduced.

The WHS Officer will also review WHS information relevant to our industry to assist the identification of workplace hazards. As new risks are identified they will be added to the Hazard Register and be assessed and treated in accordance with the WHS Program.

Reporting a Workplace Incident

When an incident may occur in the workplace which highlights the existence of a hazard but does not result in an injury (for example, a worker may fall but not be injured), the incident must be recorded in DM's **Injury/Incident Register**. The incident will be investigated and corrective action taken where this is deemed necessary.

Reviewing Workplace Injuries

It is the role of the WHS Officer to investigate all workplace injuries. Where an injury arises as the result of a hazard which has not been identified, this risk will be added to the Hazard register and be assessed and treated in accordance with the WHS Program.

Workplace Inspections

It is DM's policy to carry out workplace inspections on a regular basis to ensure we maintain a safe workplace. DM has created a program of inspections with respect to hazards that have been identified using a documented checklist. When an inspection has been completed the WHS Officer is responsible for keeping a record of the relevant inspection checklist and any subsequent Treatment Plan on file.

Hazard Risk Assessment

DM has a positive obligation to assess the risks posed by hazards in the workplace and to determine how best to modify our work processes to effectively eliminate or control the hazards.

As workplace hazards are identified they are recorded in DM's Hazard Register where each hazard is analysed. Central to the analysis process is the assessment of the **likelihood** of an event will occur, and the magnitude of the **consequences** of an event should it occur.

Using the Risk Management Standard approach documented in the **Risk Management Standard AS/NZS ISO 31000:2009,** the likelihood and consequence assessments are combined within a **risk matrix** to provide an overall assessment of risk as extreme, high, medium or low. DM can then evaluate our treatment and control options and ensure that appropriate priority is given to the treatment and control of these workplace hazards.

8.6 Record Keeping

The record keeping requirements with respect to WHS matters are set out in detail in the relevant legislation of each State and are too extensive to reproduce in full within this policy and program.

In general terms, management is responsible to ensure records are maintained with respect to all workplace safety issues, including, but not limited to:

- A copy of this program.
- Training of workers/employees.
- Minutes of WHS Committee meetings (if applicable).
- Reports on accidents, hazards and incidents.
- Reports on workplace inspections.
- Accident statistics.
- Safety equipment records including from time of purchase to ongoing maintenance.
- Method of hazard identification and risk assessments, including details of measures introduced and assessments of their effectiveness.
- Workplace safety audits and reviews.
- Details of qualifications held by key WHS and other individuals.

Many workplace safety records are confidential and should only be accessible to those who have a need to know. This is particularly important in the case of incident reports and workers compensation claims which would contain personal data relating to individuals.

8.7 Program and Policy Maintenance

Legal and Regulatory Changes

In designing our WHS and Injury Management and Return to Work programs, DM has had regard to its legal and regulatory obligations as well as to various guidelines, codes of practice and standards, published or referenced by regulators.

DM is committed to achieving best practice in workplace safety and has delegated responsibility to the WHS Officer to monitor changes in legislation and to review best practice guidelines. Our WHS Officer is provided with access to our legal representatives and industry consultants to assist in maintenance of our workplace safety programs.

Monitoring Treatments and Controls

As important as it is to identify workplace hazards, to assess them and to develop risk controls, it is critical to ensure that we monitor and review the overall effectiveness of these treatments and controls over time.

Whist all staff have an obligation to ensure that we maintain a safe workplace; it is the role of the WHS Officer to ensure the currency of the effectiveness of risk treatments and controls.

Reviewing the Workplace Safety Programs

Whilst we constantly monitor the workplace to identify hazards, DM is committed to reviewing the overall effectiveness of our Workplace Safety Programs on a regular basis.

8.8 Return to Work Program

DM Policy

It is DM policy to:

- Prevent injury and illness by providing a safe and healthy working environment.
- Ensure that return-to-work as soon as possible after an injury is normal practice and expectation.
- Ensure early access to rehabilitation services for workers who need them.
- Consult with the worker’s nominated treating doctor about return-to-work.
- Provide suitable duties, where practicable, for an injured worker.
- Consult with workers to ensure that Return-to-Work programs operate effectively.
- Ensure that participation in a Return-to-Work program will not, in itself, prejudice an injured worker.
- Participate and co-operate with our insurer’s injury management plan
- Advise workers that refusal to cooperate with an injury management plan may result in suspension of weekly benefits.
- Inform workers of their rights in relation to a workers compensation claim.
- Maintain confidentiality of rehabilitation records.
- Comply with Workplace Safety authority Guidelines if and when issued.

Procedures

When an Injury or Illness Occurs

The worker must notify the employer as soon as possible after an injury occurs. DM’s Chief Executive Officer or WH&S Officer must notify our insurer within 48 hours of a workplace injury in which the

worker is likely to be off normal duties for 7 or more days and must notify of all other workplace injuries within 7 days.

The WH&S Officer, will contact the injured worker to ensure that appropriate medical attention is received and to prepare the injured worker for a safe and timely return to work consistent with medical advice.

Nominating a Treating Doctor

The worker must nominate a Treating Doctor who will be responsible for medical management of the injury and co-operate with the development and implementation of the Return-to-Work program and Injury Management Plan.

Involving a Rehabilitation Provider

When the injured worker is not likely to resume previous duties or cannot do so without alteration to the workplace or work practices the WH&S Officer will consult with the Nominated Treating Doctor, and/or the Nominated Rehabilitation Provider to obtain assistance and guidance.
Note: The worker has the right to choose his/her own Nominated Treating Doctor and Rehabilitation Provider.

Finding Suitable Duties

The WH&S Officer in consultation with the Nominated Treating Doctor will ensure that individual return-to-work strategies are developed for each injured worker. Suitable duties for partially incapacitated workers will be meaningful, productive and consistent with remaining capabilities.

Consultation

The WH&S Officer will consult with workers prior to any arrangement for the return of an injured worker on suitable duties.

Disputes

The WH&S Officer will try to resolve disputes by consulting with the worker, the Treating Doctor and the Rehabilitation Provider.

DM's WORKERS COMPENSATION INSURER – NSW	
NAME:	**Allianz Australia Workers Compensation (NSW) Limited**
POLICY NO:	**9708163 05**
DM's WORKERS COMPENSATION INSURER – VIC	
NAME:	**Gallagher Bassett Services Workers Compensation Vic Pty Ltd**
POLICY NO:	**Employer Number: 14338195**

SCHEDULE 1 – CORPORATE CODE OF CONDUCT

1 Purpose

The purpose of this Corporate Code of Conduct is to provide a framework for decisions and actions in relation to ethical conduct in employment. It underpins the Company's commitment to integrity and fair dealing in its business affairs and to a duty of care to all employees, clients and stakeholders. The document sets out the principles covering appropriate conduct in a variety of contexts and outlines the minimum standard of behaviour expected from employees.

2 Accountabilities

2.1 Managers and Supervisors

Managers and supervisors are responsible and accountable for:

(a) undertaking their duties and behaving in a manner that is consistent with the provisions of the Code of Conduct;

(b) the effective implementation, promotion and support of the Code of Conduct in their areas of responsibility; and

(c) ensuring employees under their control understand and follow the provisions outlined in the Code of Conduct.

2.2 Employees

All employees are responsible for:

(d) undertaking their duties in a manner that is consistent with the provisions of the Code of Conduct;

(e) reporting suspected corrupt conduct; and

(f) reporting any departure from the Code of Conduct by themselves or others.

3 Personal and Professional Behaviour

When carrying out your duties, you should:

(a) behave honestly and with integrity and report other employees who are behaving dishonestly;

(b) carry out your work with integrity and to a high standard and in particular, commit to the Company's policy of producing quality goods and services;

(c) operate within the law at all times;

(d) act in the best interests of the Company;

(e) follow the policies of the Company; and

(f) act in an appropriate business-like manner when representing the Company in public forums.

4 Conflict of Interest

Potential for conflict of interest arises when it is likely that you could be influenced, or it could be perceived that you are influenced by a personal interest when carrying out your duties. Conflicts of interest that lead to biased decision making may constitute corrupt conduct.

Some situations that may give rise to a conflict of interest include situations where you have:

(i) financial interests in a matter the Company deals with or you are aware

that your friends or relatives have a financial interest in the matter;

(ii) directorships/management of outside organisations;

(iii) personal relationships with people the Company is dealing with which go beyond the level of a professional working relationship;

(iv) secondary employment, business, commercial, or other activities outside of the workplace which impacts on your duty and obligations to the Company;

(v) access to information that can be used for personal gain; and

(vi) been offered an inducement.

You may often be the only person aware of the potential for conflict. It is your responsibility to avoid any conflict from arising that could compromise your ability to perform your duties impartially. You must report any potential or actual conflicts of interest to your manager.

If you are uncertain whether a conflict exists, you should discuss that matter with your manager and attempt to resolve any conflicts that may exist.

You must not submit or accept any bribe, or other improper inducement. Any such inducements are to be reported to your manager.

5 Public and Media Comment

(a) Individuals have a right to give their opinions on political and social issues in their private capacity as members of the community.

(b) Employees must not make official comment on matters relating to the Company unless they are:

(i) authorised to do so by the Chief Executive Officer/Managing Director; or

(ii) giving evidence in court; or

(iii) otherwise authorised or required to by law.

(c) Employees must not release unpublished or privileged information unless they have the authority to do so from the Chief Executive Officer/Managing Director.

(d) The above restrictions apply except where prohibited by law, for example in relation to “whistleblowing”.

6 Use of Company Resources

Requests to use Company resources outside core business time should be referred to management for approval.

If employees are authorised to use Company resources outside core business times they must take responsibility for maintaining, replacing, and safeguarding the property and following any special directions or conditions that apply.

Employees using Company recourses without obtaining prior approval could face disciplinary and/or criminal action. Company resources are not to be used for any private commercial purposes.

7 Security of Information

Employees are to make sure that confidential and sensitive information cannot be accessed by unauthorised persons. Sensitive material should be securely stored overnight or when unattended.

Employees must ensure that confidential information is only disclosed or discussed with people who are authorised to have access to it. It is considered a serious act of misconduct to

deliberately release confidential documents or information to unauthorised persons, and may result in disciplinary action.

8 Intellectual Property/Copyright

Intellectual property (including rights relating to scientific discoveries, industrial designs, trademarks, services marks, commercial names and designations, and inventions) is valuable to the Company.

The Company is the owner of intellectual property created by employees in the course of their employment unless a specific prior agreement has been made. Employees must obtain written permission to use any such intellectual property from the Chief Executive Officer/Managing Director before making any use of that property for purpose other than as required in their role as employees.

9 Discrimination and Harassment

Employees must not harass, discriminate, or support others who harass and discriminate against colleagues or members of the public on the grounds of gender, pregnancy, marital status, age, race (including their colour, nationality, descent, ethnic or religious background), physical or intellectual impairment or sexual orientation.

Such harassment or discrimination may constitute an offence under legislation. The Company is an equal opportunity employer and managers must implement hiring procedures accordingly.

10 Corrupt Conduct

Corrupt conduct involves the dishonest or partial use of power or position which results in one person/group being advantaged over another. Corruption can take many forms including, but not limited to:

(a) official misconduct;

(b) bribery and blackmail;

(c) unauthorised use of confidential information;

(d) fraud; and

(e) theft.

Corrupt conduct will not be tolerated by the Company. Disciplinary action up to and including dismissal will be taken in the event of any employee participating in corrupt conduct.

11 Occupational Health and Safety

It is the responsibility of all employees to act in accordance with occupational health and safety legislation, regulations and policies applicable to their respective organisations and to use security and safety equipment provided.

Specifically all employees are responsible for safety in their work area by:

(a) following the safety and security directives of management;

(b) advising management of areas where there is a potential problem in safety and reporting suspicious occurrences; and

(c) minimising risks in the workplace.

12 Legislation

It is essential that all employees comply with the laws and regulations of the States in which we operate. Violations of such laws may have serious consequences for the Company and any individuals concerned. Any known violation must be reported immediately to management.

13 Fair Dealing

The Company aims to succeed through fair and honest competition and not through unethical or illegal business practices. Each employee must to deal fairly with the Company's suppliers, customers and other employees.

14 Insider Trading

All employees must observe the Company's "Security Trading Policy". In conjunction with the legal prohibition on dealing in the Company's securities when in possession of unpublished price sensitive information, the Company has established specific time periods when Directors, management and employees are permitted to buy and sell the Company's securities.

15 Responsibilities to Investors

The Company strives for full, fair and accurate disclosure of financial and other information on a timely basis.

16 Breaches of the Code of Conduct

Employees should note that breaches of certain sections of this Code of Conduct may be punishable under legislation.

Breaches of this Code of Conduct may lead to disciplinary action up to and including dismissal.

17 Reporting Matters of Concern

Employees are encouraged to raise any matters of concern in good faith with the head of their business unit or with the Chief Executive Officer/Managing Director, without fear of retribution.

SCHEDULE 2 – Leave Application Form (sample)

DirectMoney
DirectMoney Finance Pty Ltd

Address: Suite 31, Level 8, 58 Pitt Street, Sydney NSW 2000
Tel: +61 2 9252 2888 Fax: +61 2 8076 3341
Email: contact@directmoney.com.au
Web: www.directmoney.com.au
ABN: 39 119 503 221 AFSL: 458572 ACL: 458572

ANNUAL LEAVE, PERSONAL LEAVE/SICK LEAVE & LONG SERVICE LEAVE APPLICATION FORM

This form is for DirectMoney employees to use when making an application to take annual leave, personal/sick leave or long service leave.

For more information about leave entitlements and obligations, visit www.fairwork.gov.au/leave.

1. Employee's name: _____

2. Leave type

☐ Annual leave

☐ Sick leave with medical certificate (please attach to form)

☐ Personal leave/Sick leave with no medical certificate

Note: Upon termination of employment, leave taken that has not been accrued can be withheld from wages.

☐ Leave without pay ☐ Long service leave

Comments:

3. Period of leave

From:.....To:..... ("from" and "to" days are inclusive)

Total number of working days off: .....

Note: Do not include any public holidays, or substituted days in the total.

Signature of employee: _____ Date: _____ /_____/ _____

.....

4. Approval of leave *(to be completed by manager/supervisor)*

☐ Approved ☐ Not approved

Reason for refusal *(if applicable)*:_____

Name of manager: _____

Signature of manager: _____ Date:_____/_____/_____

Keep a copy of this form as a record and ensure you advise your employees if you approve or do not approve their proposed leave. You cannot unreasonably refuse an employee's request to take paid annual leave.

DirectMoney – Employee Leave Application Form [23-06-2016]

NOTE: Actual Leave Form can be downloaded from *DM's Google Drive > Company Info > Forms > Leave Forms*

SCHEDULE 3 – DM sample expense claim form (sample)

DirectMoney Expense Claim

Claimed by:		Approved by:	

Date	Payee	Detail	Account	Amount
			Total	0.00

Date Paid		Payment method	

NOTE: Actual expense claim form can be downloaded from *DM's Google Drive* > *Company Info* > *Forms* > *Expense Claims*

ACKNOWLEDGEMENT OF HR POLICY AND CONDITIONS OF EMPLOYMENT

I acknowledge that I have read and understand DM's Human Resource Policy, in particular:

- Code of Conduct (Section 5.1 on Page 5 and Schedule 1 on Pages 33-36)
- Privacy of Information (Section 5.2 on Page 10)
- Harassment (Section 5.4 on Page 11)
- Computer Use, Internet and Email Policy (Section 7 on Page 17)
- Work Health and Safety (Section 8 on Page 25)

I have been made aware how to access this policy and the DM's other policies and procedures for future reference. I am also aware that, should I be in any doubt about the interpretation of a policy or procedure, I should consult my immediate Manager or the Chief Executive Officer.

I further acknowledge that the DM's policies and conditions of employment are revised on an on-going basis and that my acknowledgement also relates to any future revisions or additions. The Company also undertakes to advise all employees of changes to policy or conditions of employment.

Signed by:

_____ (Signature)

_____ (Name in full)

_____ (Date)

This is the employee copy of the signed acknowledgement attached to your employment contract and placed on your personal file.