

prospero ™

Privacy Statement

Prospero Markets LLC

Issued on 1 September 2020
Limited Liability Company Number
533 LLC 2020

support@prosperoglobal.com
www.prosperoglobal.com

prospero ™

Content

Section A Introduction

1. INTRODUCTION.....	1
2. WHEN DOES THIS POLICY APPLY?.....	1
3. GLOSSARY.....	1

Section B Consideration of personal information privacy

4. PRIVACY STATEMENT.....	3
---------------------------	---

Section C Collection of personal information (solicited personal Information)

5. PERSONAL INFORMATION (OTHER THAN SENSITIVE INFORMATION).....	4
6. SENSITIVE INFORMATION.....	4
7. MEANS OF COLLECTION.....	5
8. INFORMATION COLLECTED BY PM.....	5
9. PURPOSE OF COLLECTION.....	5

Section D Collection of personal information (unsolicited personal Information)

10. DEALING WITH UNSOLICITED PERSONAL INFORMATION.....	7
--	---

Section E
Notification of the collection of personal information

11. NOTIFICATION OF COLLECTION.....8

Section F
Use or disclosure of personal information

12. USE OR DISCLOSURE.....9
 13. WHO DOES PM DISCLOSE PERSONAL INFORMATION TO?.10

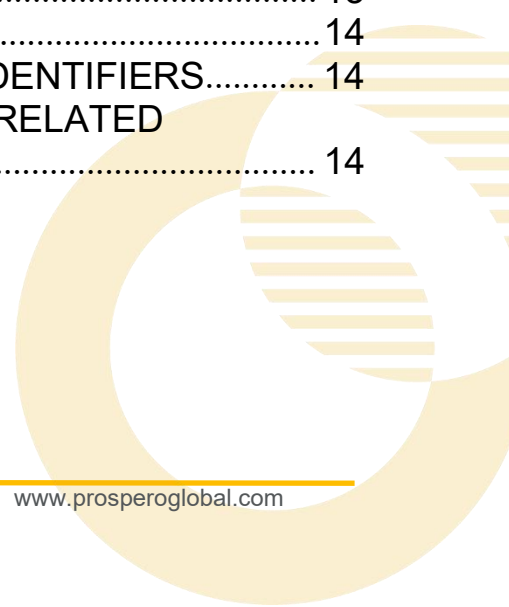
Section G
Direct marketing

14. DIRECT MARKETING..... 11
 15. EXCEPTION – PERSONAL INFORMATION OTHER THAN SENSITIVE INFORMATION.....11
 16. EXCEPTION – SENSITIVE INFORMATION..... 11
 17. REQUESTS TO STOP DIRECT MARKETING..... 12

Section H
Cross border disclosure of personal information

18. DISCLOSING PERSONAL INFORMATION TO CROSS BORDER RECIPIENTS..... 13
 Section I.....14
 19. ADOPTION OF GOVERNMENT RELATED IDENTIFIERS..... 14
 20. USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS..... 14

Section J
Integrity of personal information



21. QUALITY OF PERSONAL INFORMATION.....	15
22. SECURITY OF PERSONAL INFORMATION.....	15
23. STORAGE OF PERSONAL INFORMATION.....	15

Section K

Access to, and correction of, personal information

24. ACCESS.....	16
25. EXCEPTIONS.....	16
26. REFUSAL TO GIVE ACCESS.....	17

Section L

Correction of personal information

27. CORRECTION OF INFORMATION.....	18
28. REFUSAL TO CORRECT INFORMATION.....	18
29. REQUEST FROM A CLIENT TO ASSOCIATE A STATEMENT WITH THEIR INFORMATION.....	18
30. DEALING WITH REQUESTS.....	19

Section M

Miscellaneous

31. POLICY BREACHES.....	20
32. RETENTION OF FORMS.....	20



Section A

Introduction

1. INTRODUCTION

- 1.1 As part of Prospero Markets LLC (Limited Liability Company Number: 533 LLC 2020) herein referred to as (**Prospero Markets**) (“**PM**”) process to ensure that it continues to maintain the highest levels of professional integrity and ethical conduct, PM has adopted this Privacy Statement (“**Policy**”) to manage personal information in an open and transparent manner.
- 1.2 The provisions of this Policy will assist PM in complying with the requirements of the applicable privacy laws and principles in protecting the personal information PM holds about its clients.

2. WHEN DOES THIS POLICY APPLY?

- 2.1 This Policy applies to all representatives and employees of PM at all times and the requirements remain in force on an ongoing basis.

3. GLOSSARY

Collects

PM collects personal information only if PM collects the personal information for inclusion in a record or generally available publication.

Court/tribunal order

means an order, direction or other instrument made by:

- a. a court; or
- b. a tribunal; or
- c. a judge (including a judge acting in a personal capacity) or a person acting as a judge; or
- d. a magistrate (including a magistrate acting in a personal capacity) or a person acting as a magistrate; or
- e. a member or an officer of a tribunal;

and includes an order, direction or other instrument that is of an interim or interlocutory nature.

De-identified

personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable.

Holds

PM holds personal information if it has possession or control of a record that contains the personal information.

Identifier of an individual

means a number, letter or symbol, or a combination of any or all of those things, that is used to identify the individual or to verify the identity of the individual, but does not include:

- a. the individual's name; or
- b. the individual's business number

Personal information

means

- a. information or an opinion about an identified individual, or an individual who is reasonably identifiable;
- b. whether the information or opinion is true or not; and
- c. whether the information or opinion is recorded in a material form or not.

Sensitive information

means

- a. information or an opinion about an individual's:
 - racial or ethnic origin; or
 - political opinions; or
 - membership of a political association; or
 - religious beliefs or affiliations; or
 - philosophical beliefs; or
 - membership of a professional or trade association;
 - membership of a trade union; or
 - sexual orientation or practices; or
 - criminal record;

that is also personal information; or

- b. health information about an individual; or
- c. genetic information about an individual that is not otherwise health information.

- d. biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- e. biometric templates.

Section B

Consideration of personal information privacy

4. PRIVACY STATEMENT

- 4.1 PM's Compliance Officer ensure that at all times the provisions of this policy are implemented in the day to day running of PM.
- 4.2 The Compliance Officer must ensure that at all times this Policy:
 - a. is current and reflects the latest applicable laws; and
 - b. contains the following information:
 - the kinds of personal information that PM collects and holds;
 - how PM collects and holds personal information;
 - the purposes for which PM collects, holds, uses and discloses personal information;
 - how an individual may complain about a breach of the Privacy Principles, or other relevant legislation that binds PM, and how PM will deal with such a complaint;
 - whether PM is likely to disclose personal information to overseas recipients;
 - if PM is likely to disclose personal information to overseas recipients, the countries in which such recipients are likely to be located if it is practicable to specify those countries in this policy.
- 4.3 PM must ensure that the PM's Privacy Statement is available free of charge and in such form as appropriate. PM will make the Privacy Statement available on its website.
- 4.4 If the Privacy Statement is requested in a particular form, PM will take such steps as are reasonable to provide the Privacy Statement in the form requested.

Section C

Collection of personal information (solicited personal information)

5. PERSONAL INFORMATION (OTHER THAN SENSITIVE INFORMATION)

- 5.1 This Section C applies to the collection of personal information that is solicited by PM.
- 5.2 PM must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of PM's functions or activities.
- 5.3 PM's functions or activities include:
- a. provide financial product advice in derivatives and foreign exchange contracts;
 - b. deal in financial products including derivatives and foreign exchange contracts;
 - c. make a market in derivatives and foreign exchange contracts.

6. SENSITIVE INFORMATION

- 6.1 PM must not collect sensitive information about an individual unless:
- a. the individual consents to the collection of the information and the information is reasonably necessary for one or more of PM's functions or activities (as described in section 5.3); or
 - b. the collection of the information is required or authorised by or under an St Vincent and the Grenadines law or a Court/Tribunal order; or
 - c. a permitted general situation exists in relation to the collection of the information by PM; or
 - d. a permitted health situation exists in relation to the collection of the information by PM.

7. MEANS OF COLLECTION

- 7.1 PM must only collect personal information by lawful and fair means.
- 7.2 PM must only collect personal information about an individual from the individual (rather than someone else), unless it is unreasonable or impracticable to do so or the individual has instructed PM to liaise with someone else.
- 7.3 PM will collect personal information from an individual when:
- a. PM's Application Form is completed;
 - b. PM collects and verifies a Client's information to fulfil its obligations under the Anti Money Laundering and Counter Terrorist Financing Code;
 - c. a Client provides the information to PM's representatives over the telephone or via email;
 - d. a Client provides the information to PM on the website; and
 - e. a Client provides the information to PM via the Client Portal.

8. INFORMATION COLLECTED BY PM

- 8.1 The information PM collects may include the following:
- a. name;
 - b. date of birth;
 - c. postal or email address; or
 - d. phone numbers;
 - e. other information PM considers necessary to their functions and activities

9. PURPOSE OF COLLECTION

- 9.1 If an individual is acquiring or has acquired a product or service from PM, the individual's personal information will be collected and held for the purposes of:
- a. checking whether an individual is eligible for PM's product or service;
 - b. providing the individual with PM's product or service;
 - c. managing and administering PM's product or service;

- d. protecting against fraud, crime or other activity which may cause harm in relation to PM's products or services;
- e. complying with legislative and regulatory requirements in any jurisdiction; and
- f. to assist PM in the running of its business.

9.2 PM may also collect personal information for the purposes of letting an individual know about products or services that might better serve their needs or other opportunities in which they may be interested. Please refer to Section G for further information.



Section D

Collection of personal information (unsolicited personal Information)

10. DEALING WITH UNSOLICITED PERSONAL INFORMATION

10.1 If PM:

- a. receives personal information about an individual; and
- b. the information is not solicited by PM,

PM must, within a reasonable period after receiving the information, determine whether or not it was permitted to collect the information under Section C above.

10.2 PM may use or disclose the personal information for the purposes of making the determination under paragraph 10.1.

10.3 If PM determines that it could not have collected the personal information, PM must as soon as practicable, destroy the information or ensure that the information is de-identified, only if it is lawful and reasonable to do so.

Section E

Notification of the collection of personal information

11. NOTIFICATION OF COLLECTION

- 11.1 This section 11 applies to:
- a. solicited information; and
 - b. unsolicited information to which section 10 does not apply
- 11.2 PM must notify the individual of the following matters in the Privacy Statement:
- a. PM's identity and contact details;
 - b. if PM collects the personal information from a third party or the individual is not aware that PM has collected the personal information, the fact that PM so collects, or has collected the information and the circumstances of that collection;
 - c. if the collection of the personal information is required or authorised by or under an St Vincent and the Grenadines law or a Court/Tribunal order, the fact that the collection is so required or authorised (including the details of the law or court);
 - d. the purposes for which PM collects the personal information;
 - e. the main consequences (if any) for the individual if the information is not collected by PM;
 - f. any other entities to which PM usually discloses personal information of the kind collected by PM;
 - g. that PM's Privacy Statement and this Privacy Statement contains information about how the individual may access the personal information about the individual that is held by PM and seek correction of such information;
 - h. whether PM will disclose the personal information to overseas recipients; and
 - i. if PM discloses the personal information to overseas recipients, the countries in which such recipients will be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Section F

Use or disclosure of personal information

12. USE OR DISCLOSURE

- 12.1 Where PM holds personal information about an individual that was collected for a particular purpose (“the primary purpose”), PM must not use or disclose the information for another purpose (“the secondary purpose”) unless:
- a. the individual has consented to the use or disclosure of the information; or
 - b. the individual would reasonably expect PM to use or disclose the information for the secondary purpose and the secondary purpose is:
 - directly related to the primary purpose (if the information is sensitive information); or
 - related to the primary purpose (if the information is not sensitive information);
 - a permitted general situation exists in relation to the use or disclosure of the information by PM; or
 - PM reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.
- 12.2 Where PM uses or discloses personal information in accordance with section 12, PM will keep a copy of this disclosure (eg: the email or letter used to do so).
- 12.3 This section 12 does not apply to:
- a. personal information for the purposes of direct marketing; or
 - b. government related identifiers.
- 12.4 If PM collects personal information from a related body corporate, this section 12 applies as if PM’s primary purpose for the collection was the primary purpose for which the related body corporate collected the information.

13. WHO DOES PM DISCLOSE PERSONAL INFORMATION TO?

- 13.1 PM may disclose personal information collected from clients and prospective clients to the following:
- a. organisations involved in providing, managing or administering PM's product or service such as third party suppliers, e.g. printers, posting services, and our advisers;
 - b. organisations involved in maintaining, reviewing and developing PM's business systems, procedures and infrastructure, including testing or upgrading PM's computer systems;
 - c. organisations involved in a corporate re-organisation;
 - d. Organisations that PM outsources its AML/CTF obligations to, including organisations that conduct background checks;
 - e. organisations involved in the payments system, including financial institutions, merchants and payment organisations;
 - f. organisations involved in product planning and development;
 - g. other organisations, who jointly with PM, provide its products or services;
 - h. authorised representatives who provide PM's products or services on its behalf;
 - i. the individual's representatives, including your legal advisers;
 - j. debt collectors;
 - k. PM's financial advisers, legal advisers or auditors;
 - l. fraud bureaus or other organisations to identify, investigate or prevent fraud or other misconduct;
 - m. external dispute resolution schemes; or
 - n. regulatory bodies, government agencies and law enforcement bodies in any jurisdiction.

Section G

Direct marketing

14. DIRECT MARKETING

- 14.1 PM must not use or disclose the personal information it holds about an individual for the purpose of direct marketing.

15. EXCEPTION – PERSONAL INFORMATION OTHER THAN SENSITIVE INFORMATION

- 15.1 PM may use or disclose personal information (other than sensitive information) about an individual for the purposes of direct marketing if:
- a. PM collected the information from the individual; and the individual would reasonably expect PM to use or disclose the information for that purpose; or
 - b. PM has collected the information from a third party; and either:
 - PM has obtained the individual's consent to the use or disclose the information for the purpose of direct marketing; or
 - it is impracticable for PM to obtain the individual's consent; and
 - c. in each direct marketing communication with the individual PM:
 - includes a prominent statement that the individual may make such a request; or
 - directs the individual's attention to the fact that the individual may make such a request; and
 - d. the individual has not made such a request.

16. EXCEPTION – SENSITIVE INFORMATION

- 16.1 PM may use or disclose sensitive information about an individual for the purpose of direct marketing if the individual has consented to the use or disclosure of the information for that purpose.

17. REQUESTS TO STOP DIRECT MARKETING

- 17.1 Where PM uses or discloses personal information about an individual for the purposes of direct marketing by PM or facilitating direct marketing by another organisation, the individual may request:
- a. that PM no longer provide them with direct marketing communications;
 - b. that PM does not use or disclose the individual's personal information for the purpose of facilitating direct marketing by another organisation;
 - c. that PM provides the source of the personal information.
- 17.2 Where PM receives a request from an individual under section 17.1, PM will:
- a. give effect to the request under section 17.1(a) or 17.1(b) within a reasonable period after the request is made and free of charge; and
 - b. notify the individual of the source of the information, if the individual requests it, unless it is impracticable or unreasonable to do so.
- 17.3 This Section G does not apply to the extent that the following laws apply:
- a. the Do Not Call Register;
 - b. the Spam Act; or
 - c. any other Act.

Section H

Cross border disclosure of personal information

18. DISCLOSING PERSONAL INFORMATION TO CROSS BORDER RECIPIENTS

- 18.1 Where PM discloses personal information about an individual to a recipient who is not in St Vincent and the Grenadines and who is not PM or the individual, PM must ensure that the overseas recipient does not breach our Privacy Principles.
- 18.2 The countries we may disclose an individual's personal information to include:
- a. China mainland;
 - b. Hong Kong; and
 - c. New Zealand.
- 18.3 Section 18.1 does not apply where:
- a. PM reasonably believes that:
 - information is subject to a law or binding scheme that has the effect of protecting the information in a way that is at least substantially similar to the way in which our Privacy Principles protect the information; and
 - there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or
 - b. both of the following apply:
 - PM has informed the individual that if they consent to the disclosure of information PM will not take reasonable steps to ensure the overseas recipient does not breach our Privacy Principles; and
 - after being so informed, the individual consents to disclosure;
 - c. the disclosure of the information is required or authorised by or under a St Vincent and the Grenadines law or a Court/Tribunal order; or
 - d. a permitted general situation exists in relation to the disclosure of the information by PM.

Section I

Adoption, use or disclosure of government identifiers

19. ADOPTION OF GOVERNMENT RELATED IDENTIFIERS

19.1 PM must not adopt a government related identifier of an individual as its own identifier unless:

- a. PM is required or authorised by or under a St Vincent and the Grenadines law or a Court/Tribunal order to do so; or
- b. the identifier, PM and the circumstances of the adoption are prescribed by regulations.

20. USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS

20.1 Before using or disclosing a government related identifier of an individual, PM must ensure that such use or disclosure is:

- a. reasonably necessary for PM to verify the identity of the individual for the purposes of the organisation's activities or functions; or
- b. reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority; or
- c. required or authorised by or under an St Vincent and the Grenadines law or a Court/Tribunal order; or
- d. within a permitted general situation (other than the situation referred to in the applicable privacy laws and principles; or
- e. reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- f. the identifier, PM and the circumstances of the adoption are prescribed by regulations.

Section J

Integrity of personal information

21. QUALITY OF PERSONAL INFORMATION

- 21.1 PM will ensure that the personal information it collects and the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up to date, complete and relevant.

22. SECURITY OF PERSONAL INFORMATION

- 22.1 PM will ensure that it protects any personal information it holds from misuse, interference, loss, unauthorised access, modification and disclosure.
- 22.2 PM will take reasonable steps to destroy or de-identify any personal information it holds where:
- PM no longer needs the personal information for any purpose for which the information may be used or disclosed by PM;
 - PM is not required to retain that information under a St Vincent and the Grenadines law, or a Court/Tribunal order.

23. STORAGE OF PERSONAL INFORMATION

- 23.1 PM stores personal information in different ways, including:
- hard copy on site at PMs head office; and
 - electronically secure data centres owned by either PM or external service providers.

In order to ensure PM protects any personal information it holds from misuse, interference, loss, unauthorised access, modification and disclosure, PM implements the following procedure/system:

- access to information systems is controlled through identity and access management;
- employees are bound by internal information securities policies and are required to keep information secure;
- all employees are required to complete training about information security; and

- d. PM regularly monitors and reviews its compliance with internal policies and industry best practice.

Section K

Access to, and correction of, personal information

24. ACCESS

- 24.1 PM must give an individual access to the personal information it holds about the individual if so requested by the individual.
- 24.2 PM must respond to any request for access to personal information within a reasonable period after the request is made.
- 24.3 PM must give access to the information in the manner requested by the individual, if it is reasonable and practicable to do so and must take such steps as are reasonable in the circumstances to give access in a way that meets the needs of PM and the individual.
- 24.4 PM must not charge an individual for making a request, and must not impose excessive charges for the individual to access their personal information.

25. EXCEPTIONS

- 25.1 PM is not required to give an individual access to their personal information if:
 - a. PM reasonably believes that giving access would pose a serious threat to the life, health or safety of any individual, or to public health or public safety; or
 - b. giving access would have an unreasonable impact on the privacy of other individuals; or
 - c. the request for access is frivolous or vexatious; or
 - d. the information relates to existing or anticipated legal proceedings between PM and the individual, and would not be accessible by the process of discovery in those proceedings; or
 - e. giving access would reveal intentions of PM in relation to negotiations with the individual in such a way as to prejudice those negotiations; or
 - f. giving access would be unlawful; or

- g. denying access is required or authorised by or under a St Vincent and the Grenadines law or a Court/Tribunal order; or
- h. PM has reason that unlawful activity, or misconduct of a serious nature, that relates to our functions or activities has been, or may be engaged in and giving access would be likely to prejudice the taking of appropriate action in relation to the matter; or
- i. giving access would be likely to prejudice one or more enforcement related activities conducted by, or on behalf of, an enforcement body; or
- j. giving access would reveal evaluative information generated within PM in connection with a commercially sensitive decision-making process.

26. REFUSAL TO GIVE ACCESS

26.1 If PM refuses to give access in accordance with section 24 or to give access in the manner requested by the individual, PM will give the individual a written notice that sets out:

- a. the reasons for the refusal except to the extent that, having regard to the grounds for the refusal, it would be unreasonable to do so; and
- b. the mechanisms available to complain about the refusal; and
- c. any other matter prescribed by the regulations.

26.2 Where PM refuses to give access under section 25.1(j) PM may include an explanation of the commercially sensitive decision in its written notice of the reasons for denial.

Section L

Correction of personal information

27. CORRECTION OF INFORMATION

- 27.1 PM must take reasonable steps to correct all personal information, having regard to the purpose for which the information is held where:
- a. PM is satisfied the information is inaccurate, out of date, incomplete, irrelevant or misleading; or
 - b. the individual requests PM corrects the information.
- 27.2 Where PM corrects personal information about an individual that PM previously disclosed to another entity and the individual requests PM to notify the other entity of the correction, PM must take reasonable steps to give that notification, unless it is impracticable or unlawful to do so.

28. REFUSAL TO CORRECT INFORMATION

- 28.1 If PM refuses to correct personal information as requested by the individual, PM will give the individual a written notice that sets out:
- a. the reasons for the refusal except to the extent that it would be unreasonable to do so; and
 - b. the mechanisms available to complain about the refusal; and
 - c. any other matter prescribed by the regulations.

29. REQUEST FROM A CLIENT TO ASSOCIATE A STATEMENT WITH THEIR INFORMATION

- 29.1 If:
- a. PM refuses to correct personal information as requested by the individual; and
 - b. the individual requests that PM associate a statement noting that the information is inaccurate, out of date, incomplete, irrelevant or misleading, with the individual's information.

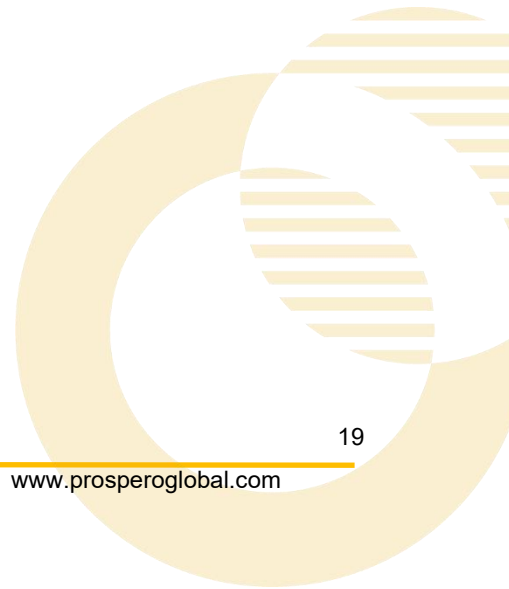
PM must take such steps as are reasonable in the circumstances to associate

the statement (as described in section 30.1(b)) with the individual's personal information. The statement should be associated with the information in such a way that will make the statement apparent to users of the information.

30. DEALING WITH REQUESTS

30.1 PM must:

- a. respond to requests under this Section L within a reasonable period after the request is made; and
- b. must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information.



Section M

Miscellaneous

31. POLICY BREACHES

- 31.1 Breaches of this Policy may lead to disciplinary action being taken against the relevant party, including dismissal in serious cases and may also result in prosecution under the law where that act is illegal. This may include re-assessment of bonus qualification, termination of employment and/or fines (in accordance with the applicable privacy laws and principles).
- 31.2 Staff are trained internally on compliance and their regulatory obligation to PM. They are encouraged to respond appropriately to, and report all breaches of the law and other incidents of non-compliance, including PM's policies, and seek guidance if they are unsure.
- 31.3 Staff must report breaches of this Policy directly to the Compliance Officer.

32. RETENTION OF FORMS

- 32.1 The Compliance Officer will retain the completed forms for seven (7) years in accordance with PM's Document Retention Policy. The completed forms are retained for future reference and review.
- 32.2 As part of their training, all staff are made aware of the need to practice thorough and up to date record keeping, not only as a way of meeting PM's compliance obligations, but as a way of minimising risk.