DATA PROTECTION POLICY

GET SACE POINTS

Index

DATA PROTECTION POLICY

DATA PROTECTION POLICY

PART I – INTRODUCTORY

This Part I sets out the interpretation of this Policy, the scope thereof, and provides an overview of the manner in which Get SACE Points collects and processes personal information.

1 INTERPRETATION

In this Policy, unless inconsistent with or otherwise indicated by the context –

1.1 "**the Act**" means the Protection of Personal Information Act, No. 4 of 2013;

1.2 "**Employee**" means any employee of Get SACE Points responsible or charged with the processing of personal information in the performance of his duties or functions;

1.3 "**Get SACE Points**" means Learndirect Training Solutions (Pty) Ltd, registration number 2011/006110/07, a private company with limited liability duly incorporated in accordance with the laws of the Republic of South Africa, trading as Get SACE Points;

1.4 "**Information Officer**" means the information officer of Get SACE Points appointed in terms of the Act, being the person indicated in clause 45.8;

1.5 "**Operator**" means a person who processes personal information for a Responsible Party in terms of a contract or mandate, without coming under the direct authority of that party;

1.6 "**the Policy**" means the data protection policy set out in this document, as amended from time to time;

1.7 "**Responsible Party**" means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information;

1.8 "**Subject**" means any person whose personal information is processed by Get SACE Points, including but not limited to clients or customers of Get SACE Points and any Get SACE Points employee, director, shareholder, or service provider;

1.9 words and phrases defined in the Act shall bear the same meaning as set out herein;

1.10 words importing the singular shall include the plural and vice versa;

1.11 words importing natural persons includes legal persons and partnerships and vice versa;

1.12 words importing the one gender includes the other genders;

1.13 the *eiusdem generis* rule shall not apply and whenever a term is followed by the word "including" which is then followed by specific examples, such examples shall not be construed so as to limit the meaning of that term;

1.14 any reference to an enactment is to that enactment as at the publication hereof and as amended or re-enacted from time to time; and

1.15 where figures are referred to in numerals and in words, if there is any conflict between the two, the words shall prevail.

2 PURPOSE OF THIS POLICY

The purpose of this Policy is to ensure that all Employees are aware of Get SACE Points' responsibilities in terms of the Act, their responsibilities towards Get SACE Points, and the procedures in place for the processing of personal information.

3 COLLECTION AND PROCESSING OF PERSONAL INFORMATION

Get SACE Points collects and processes personal information belonging to Subjects in order to carry out and pursue its business and related operational interests. The purposes for such collection and processing includes but is not limited to the following -

3.1 recruitment and employment purposes;

3.2 confirming, verifying, and updating personal details;

3.3 capture data for the provision of services to educational institutions, schools, and educational professionals, and teachers;

3.4 in respect of suppliers and service providers;

3.5 contracts and business transactions; and

3.6 assessing and processing queries, enquiries and complaints;

4 SCOPE

This Policy shall bind all Employees, contractors, vendors and any other third parties entrusted with processing of personal information on behalf of Get SACE Points. Insofar as written acceptance of this Policy is required, Get SACE Points shall ensure that such written acceptance is obtained from the relevant individual or entity.

PART II – PROCESSING

5 DATA PROTECTION CONDITIONS

This Part II sets out the general principles to be adhered to in respect of the processing of personal information by Get SACE Points, including but not limited to the 8 data protection conditions set out under section 4 of the Act, which are as follows -

5.1 personal information shall be obtained and processed fairly and lawfully;

5.2 personal information shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes, unless specific consent to do so has been obtained;

5.3 personal information shall be adequate, relevant, and not excessive in relation to the purpose or purposes for which they are processed;

5.4 personal information shall be accurate and, where necessary, kept up to date;

5.5 personal information processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes;

5.6 personal information shall be processed in accordance with the rights of Subjects under the Act;

5.7 appropriate technical and organisational safeguards and measures shall be put in place to protect and guard against unauthorised or unlawful processing of personal information and against accidental loss or destruction of, or damage to, personal information; and

5.8 personal information shall not be transferred outside South Africa to another country unless the Subject has provided his consent and further provided that, that country has similar data privacy laws to those provided for in the Act in place, or the person to whom the personal information is being transferred provides a written undertaking to apply the principles provided in the Act to the processing of the aforementioned personal information.

6 PERSONAL INFORMATION AND PROCESSING

6.1 Personal information is information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to –

6.1.1 information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;

6.1.2 information relating to the education or the medical, financial, criminal or employment history of the person;

6.1.3 any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;

6.1.4 the biometric information of the person;

6.1.5 the personal opinions, views, or preferences of the person;

6.1.6 correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence;

6.1.7 the views or opinions of another individual about the person; and

6.1.8 the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

6.2 The processing of personal information is any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including –

6.2.1 the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;

6.2.2 dissemination by means of transmission, distribution, or making available in any other form; or

6.2.3 merging, linking, as well as restriction, degradation, erasure, or destruction of information.

7 ACCOUNTABILITY

7.1 Get SACE Points is a Responsible Party in terms of the Act because it, alone or in conjunction with others, determine the purpose of and means for processing personal information. Get SACE Points must accordingly comply with the provisions of the Act when processing personal information.

7.2 Get SACE Points may also be an Operator in terms of the Act which processes personal information for a Responsible Party, in terms of an agreement with such Responsible Party, without coming under the direct authority of that Responsible Party.

7.3 The measures set out herein must be complied with at the time of determining the purpose and means of processing and during the processing of personal information.

8 NOTICE TO THE SUBJECT

8.1 Before any personal information is processed, the Employee must bring to the Subject's attention the provisions of the privacy policy of Get SACE Points. Get SACE Points' privacy policy shall be contained on Get SACE Points' website and/or included as a provision of the agreements entered into with Subjects and/or delivered to the Subject as a separate document. In addition to Get SACE Points' general privacy policy, the notice to the Subject shall include the information set out in clause 16.

8.2 When processing a Subject's personal information, an Employee must ensure that -

8.2.1 they only process personal information, which is relevant and accurate and only for the purpose for which it is required; and

8.2.2 special personal information will only be processed in line with the provisions set out under the Act and in accordance with instructions set out by the Information Officer from time to time, as explained in more detail in 18 below.

9 PROCESSING LIMITATION

9.1 Get SACE Points processes personal information where it is necessary to do so in the performance of its obligations to its Subjects.

9.2 The “Subjects” include –

9.2.1 Subjects who have entered into an agreement with Get SACE Points or to whom Get SACE Points provides services; and

9.2.2 Subjects that have entered into agreements with data subjects and who have in turn appointed Get SACE Points as a service provider to perform services in terms of such agreement.

9.3 Get SACE Points will also process information if –

9.3.1 the Subject (or a competent person where the Subject is a child) consents to the processing;

9.3.2 processing complies with an obligation imposed by law on Get SACE Points;

9.3.3 processing protects a legitimate interest of the Subject;

9.3.4 processing is necessary for the proper performance of a public law duty by a public body; or

9.3.5 processing is necessary for pursuing the legitimate interests of Get SACE Points or of a third party to whom the information is supplied.

9.4 Before processing of personal information, the Employee must ensure that at least one of the factors in 9.1 or 9.3 above are present.

10 COLLECTION OF PERSONAL INFORMATION

10.1 Get SACE Points collects personal information from the Subject.

10.2 If the personal information is not collected directly from the Subject –

10.2.1 the third party from whom the information is collected must have obtained the consent of the Subject (or of a competent person where the Subject is a child) to the collection of the information from the third party; or

10.2.2 the collection of the personal information must otherwise be authorised in terms of the Act.

10.3 Get SACE Points may also collect personal information if any of the circumstances in section 12(2) of the Act are present at the time of collection of the personal information, being -

10.3.1 the personal information is contained in or derived from a public record or has been deliberately made public by the Subject;

10.3.2 the Subject has consented to the collection of the information from another source;

10.3.3 collection of personal information from another source would not prejudice the interests of the Subject; or

10.3.4 collection of the personal information from another source is necessary to maintain the legitimate interest of Get SACE Points or of a third party to whom the information is supplied.

10.4 Before collecting personal information, the Employee must ensure that the personal information is being collected from the Subject or that the third party has confirmed that it has obtained the consent of the Subject.

11 PURPOSE SPECIFICATION

11.1 Get SACE Points will only retain records of personal information –

11.1.1 for as long as it is necessary to perform its obligations to Subjects;

11.1.2 if retention of the record is required or authorised by law;

11.1.3 if Get SACE Points reasonably requires the record for lawful purposes related to its functions or activities;

11.1.4 if retention of the record is required by a contract between the parties thereto; or

11.1.5 if the Subject, or a competent person where the Subject is a child, has consented to the retention of the record; or

11.1.6 if retention is required for historical, statistical or research purposes, provided that Get SACE Points has established appropriate safeguards against the records being used for any other purposes.

11.2 Get SACE Points will destroy or delete records of the personal information or de-identify the personal information as soon as reasonably practical after the circumstances in clause 11.1 no longer exist or as otherwise requested by a Subject in terms of the provisions of this Policy.

12 RESTRICTION ON PROCESSING

12.1 Get SACE Points will restrict processing of personal information if –

12.1.1 its accuracy is contested by the Subject, for a period enabling Get SACE Points to verify the accuracy of the information;

12.1.2 Get SACE Points no longer needs the personal information for achieving the purpose for which the information was collected or subsequently processed, but it has to be maintained for purposes of proof;

12.1.3 the processing is unlawful, and the Subject opposes its destruction or deletion and requests the restriction of its use instead; or

12.1.4 the Subject requests to transmit the personal information into another automated processing system.

12.2 A restriction on processing of personal information referred to above means that such personal information will only be processed –

12.2.1 for storage purposes;

12.2.2 for purposes of proof;

12.2.3 with the Subject's consent, or with the consent of a competent person if the Subject is a child; or

12.2.4 for the protection of the rights of another natural or legal person or if such processing is in the public interest.

12.3 If a restriction is placed on the processing of personal information as aforesaid, Get SACE Points will endorse the records of personal information accordingly or will otherwise notify the Employees of such restriction.

12.4 When processing personal information, the Employee must ensure that none of the circumstances in clause 12.1 are present and that there is no restriction on the processing of information as set out in clause 12.2.

13 LIMITATION ON FURTHER PROCESSING

13.1 After the collection of the personal information Get SACE Points will only process personal information in a manner compatible with the purpose for which the personal information was collected. Further processing of personal information will be done only when necessary to perform Get SACE Points' obligations to its Subjects or otherwise in accordance with the provisions of the Act.

13.2 When processing personal information after it is collected, Employees must have due regard for the purpose for which the personal information was collected.

14 INFORMATION QUALITY

14.1 Having regard for the purpose for which personal information is collected, Get SACE Points will take reasonably practical steps to ensure that the personal information is complete, accurate, not misleading, and updated, where necessary.

14.2 When collecting personal information from the Subject, the Employee must ask the Subject to confirm the correctness and completeness of the personal information.

14.3 All fillable forms, agreements, or other documents presented to Subjects for completion must include a confirmation that the personal information is correct, complete, and accurate.

15 OPENNESS

15.1 Get SACE Points maintains documentation of its processing operations as required in terms of sections 14 to 51 of the Promotion of Access to Information Act No. 2 of 2000.

15.2 When collecting personal information directly from the Subject, Get SACE Points must notify the Subject of –

15.2.1 the information being collected;

15.2.2 Get SACE Points' name and address (which name and address must be included on any fillable forms, documents or agreements applicable to the Subject);

15.2.3 the purpose for which the information is being collected;

15.2.4 whether or not the supply of the information by that Subject is voluntary or mandatory;

15.2.5 the consequences of the failure to provide the information;

15.2.6 any particular law authorising or requiring the collection of the information;

15.2.7 if applicable, the fact that Get SACE Points intends to transfer the information to a third party country or international organisation and the level of protection afforded to the information by country or international organisation;

15.2.8 any further information which is necessary, having regard to the specific circumstances in which the information is or is not to be processed, to enable processing in respect of the Subject to be reasonable, including –

15.2.8.1 recipient or category of recipients of the information;

15.2.8.2 nature or category of the information;

15.2.8.3 existence of the right of access to and the right to rectify the information collected;

15.2.8.4 existence of the right to object to the processing of personal information as referred to in section 11(3) of the Act; and

15.2.8.5 right to lodge a complaint to the Information Regulator and the contact details of the Information Regulator.

15.3 If the personal information is not collected from the Subject, Get SACE Points will obtain written confirmation from the third party that it has taken the steps contemplated in clause 15.2.

15.4 Before processing personal information, the Employee must ensure that the record of personal information is endorsed with confirmation that Get SACE Points has complied with clause 15.2 or 15.3, as the case may be.

16 PROCESSING PERSONAL INFORMATION AS AN OPERATOR

16.1 If Get SACE Points processes personal information as an Operator or otherwise on behalf of a third party, Get SACE Points will –

16.1.1 enter into a written agreement with the third party in respect of its appointment to process information on behalf of the third party;

16.1.2 only process such information in the course of performance or its duties to the third party or as otherwise required by law; and

16.1.3 notify the third party immediately where there are reasonable grounds to believe that the personal information has been accessed or acquired by an unauthorised person.

16.2 A third party may not process personal information on behalf of Get SACE Points, other than in the manner set out in clause 22.

16.3 The Employee must distinguish between the circumstances in which Get SACE Points processes information as an Operator and the circumstances in which Get SACE Points processes information as a Responsible Party.

17 ACCESS TO AND CORRECTION OF PERSONAL INFORMATION

17.1 Get SACE Points will provide a Subject with access to the personal information in respect of that Subject held by Get SACE Points, provided that –

17.1.1 the Subject submits a written application for such access in such reasonable form and manner prescribed by Get SACE Points; and

17.1.2 the Subject makes payment of a prescribed fee.

17.2 Get SACE Points may or must, as required in terms of applicable laws, refuse access to such records requested by the Subject, to the extent that such records are prevented from being accessed on grounds set out in Chapter 4 of Part 2 and Chapter 4 of Part 3 of the Promotion of Access to Information Act No. 2 of 2000.

17.3 If Get SACE Points makes information available following a request by a Subject, Get SACE Points will notify the Subject of the Subject's right to request the correction of the information.

17.4 If a Subject requests that Get SACE Points –

17.4.1 corrects or deletes personal information about the Subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully; or

17.4.2 destroys or deletes a record of personal information about the Subject that Get SACE Points is no longer authorised to retain in terms of the Act,

the provisions of clause 25 shall be applicable.

18 SPECIAL PERSONAL INFORMATION

18.1 Get SACE Points occasionally processes personal information concerning the race, ethnicity, or the criminal history of a Subject.

18.2 Get SACE Points will only process such special personal information in compliance with the relevant provisions of sections 27 to 31 of the Act.

18.3 Insofar as Get SACE Points processes special personal information relating to a Subject's race, ethnicity or criminal behaviour or records, such processing shall be done with the consent of the Subject, in writing.

19 PROCESSING OF INFORMATION OF CHILDREN

Get SACE Points will only process personal information if the processing is carried out –

19.1 with the prior consent of a competent person; or

19.2 as otherwise permitted in terms of section 35(1) of the Act.

20 DIRECT MARKETING

20.1 Get SACE Points may process personal information for the purpose of direct marketing.

20.2 Get SACE Points shall not process personal information of a Subject for the purpose of direct marketing by means of any form of electronic communication, including automatic calling machines, facsimile machines, SMSs, or e-mail unless –

20.2.1 the Subject has given his, her, or its consent to the processing; or

20.2.2 the Subject is a client of Get SACE Points.

20.3 Get SACE Point shall only be entitled to request the consent of a Subject required in accordance with clause 20.2.1 once, provided that such Subject has not previously withheld such consent.

20.4 Get SACE Points may only undertake direct marketing pursuant to clause 20.2.2 –

20.4.1 if Get SACE Points has obtained the Subject's contact details in the context of the sale of a product or service;

20.4.2 for the purpose of direct marketing of Get SACE Points' own similar products or services; and

20.4.3 provided that the Subject was given a reasonable opportunity to object, free of charge and with ease to such use of his details -

20.4.3.1 at the time when the personal information was initially collected; and

20.4.3.2 on the occasion of each communication thereafter.

20.5 Any direct marketing communication must contain Get SACE Points' identity and contact details.

21 AUTOMATED DECISION MAKING

A Subject will not be subject to a decision which results in legal consequences for him, her or it, or which affects him, her or it to a substantial degree, which is based solely on the basis of the automated processing of personal information intended to provide a profile of such person including his or her performance at work, or his, her or its credit worthiness, reliability, location, health, personal preferences, or conduct, unless the decision has been taken in connection with the conclusion or execution of a contract, and -

21.1 the request of the Subject in terms of the contract has been met;

21.2 appropriate measures have been taken to protect the Subject's legitimate interests; or

21.3 is governed by a law or code of conduct in which appropriate measures are specified for protecting the legitimate interests of Subjects.

PART III – SHARING OF INFORMATION

This Part III sets out the manner in which Get SACE Points may share personal information with Operators, across borders, and within Get SACE Points.

22 SHARING OF PERSONAL INFORMATION WITH OPERATORS

If Get SACE Points appoints an Operator to process personal information on its behalf Get SACE Points shall -

22.1 enter into a written agreement with the Operator in respect of such appointment;

22.2 ensure that the Operator maintains adequate security measures referred to in section 19 of the Act; and

22.3 remain responsible to comply with the provisions of this Policy and the Act.

23 TRANSBORDER INFORMATION FLOWS

Get SACE Points will not transfer personal information to a third party who is in a foreign country unless either the circumstances set out in either clauses 23.1 or 23.2 are applicable.

23.1 Consent

23.1.1 The recipient of the information is subject to a law, binding corporate rules or binding agreement which provides an adequate level of protection that –

23.1.1.1 effectively upholds principles for the reasonable processing of the information, that are substantially similar to the conditions for the lawful processing of personal information relating to a Subject;

23.1.1.2 includes provisions, consistent with the Act, regarding the further transfer of personal information from the recipient to third parties who are in a foreign country;

23.1.2 the Subject consents to the transfer;

23.1.3 the transfer is necessary for the performance of a contract between the Subject and Get SACE Points, or for the implementation of pre-contractual measures taken in response to the Subject's request; and

23.1.4 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Subject between Get SACE Points and a third party.

23.2 Benefit of the Subject

The transfer is for the benefit of the Subject, and –

23.2.1 it is not reasonably practicable to obtain the consent of the Subject to that transfer; and

23.2.2 if it were reasonably practicable to obtain such consent, the Subject would be likely to give it.

24 SHARING OF PERSONAL INFORMATION

All transfer of personal information to an entity outside of Get SACE Points must be associated with a written contract or non-disclosure agreement or be in terms of a specified protocol or in terms of an applicable law. No personal information may be provided to anyone outside Get SACE Points, without the written approval of the Information Officer in respect of a specific instance, or in respect of a general process or category of information.

PART IV – CORRECTION, DESTRUCTION, DELETION, DISPOSAL AND RETENTION

This Part IV sets out the processes for the correction, destruction, deletion, disposal, and retention of personal information.

25 CORRECTION OR DELETION OF INFORMATION

25.1 Upon receiving a request in accordance with clause 17.1, Get SACE Points must, as soon as reasonably practicable follow the steps set out in 25.1.1 and 25.1.2.

25.1.1 Correction or Deletion

Get SACE Points shall -

25.1.1.1 correct the information; or

25.1.1.2 destroy or delete the information,

as agreed with the Subjects.

25.1.2 Steps Taken

Get SACE Points shall -

25.1.2.1 provide the Subject, to his or her satisfaction, with credible evidence in support of the correction or deletion of the personal information; or

25.1.2.2 where agreement cannot be reached between Get SACE Points and the Subject regarding the steps to be taken in respect of the correction or deletion of the personal information, Get SACE Points shall such steps as are reasonable in the circumstances to attach to the information in such a manner that it will always be read with the information, an indication that a correction of the information has been requested but has not been made.

25.2 If Get SACE Points takes steps that result in a change to the information and the changed information has an impact on decisions that have been or will be taken in respect of the Subject in question, Get SACE Points will, if reasonably

practicable, inform each person or body or Responsible Party to whom the personal information has been disclosed of those steps.

25.3 Get SACE Points must notify a Subject, who has made a request as aforesaid, of the action taken as a result of the request.

26 DISPOSAL OF PAPER AND/OR EXTERNAL MEDIA

26.1 All paper which contains personal information that is no longer needed must be shredded before being disposed. Employees may not place such documents in a trash container without first shredding.

26.2 Employees may not throw any media containing personal information in the trash without taking steps to ensure the personal information is appropriately destroyed.

27 RETENTION / DESTRUCTION OF INFORMATION

27.1 Notwithstanding anything to the contrary contained herein, personal information shall only be retained for so long as it is required by Get SACE Points to conduct its business or in terms of any applicable laws.

27.2 A register shall be maintained of the personal information destroyed (if not destroyed in accordance with a specific destruction protocol) which shall include the following information -

27.2.1 the responsible Employee attending to the destruction;

27.2.2 the type of document or information being destroyed;

27.2.3 the reason for the destruction; and

27.2.4 a copy of the written authorisation for the destruction provided by the Information Officer.

PART V – EMPLOYEE USE POLICY AND SECURITY MEASURES

This Part V sets out security measures specific to Employees of Get SACE Points, which are put in place in order to protect the personal information. This Part V further sets out Get SACE Points' policy relating to the use of its resources.

28 GENERAL USE

28.1 Employees must lock unattended devices when leaving the work area and any paper or hard copies of personal information and portable electronic devices containing personal information should be securely stored, preferably in locked units, and must not be left on desks overnight or in view of other Employees or third parties.

28.2 Employees may only connect or install computer hardware and software owned by and installed by Get SACE Points on Get SACE Points' equipment or network.

28.3 Employees may only use the computers supplied by Get SACE Points, alternatively (if authorised by the Information Officer) computers with a specific business profile for purposes of Get SACE Points' business and in fulfilling their duties to Get SACE Points. Employees may not make modification or configuration changes on computers supplied by Get SACE Points for home use.

28.4 All software programs and documentation generated or provided by Employees, consultants, or contractors for the benefit of Get SACE Points are the property of Get SACE Points, unless otherwise agreed by Get SACE Points in writing.

29 PORTABLE MEDIA DEVICES

The following rules apply to the use of portable media devices (USB, CDs, etc.) -

29.1 Employees and IT personnel must ensure that all external or portable media devices are be scanned for virus infections prior to connecting to or copying information to a Get SACE Points computer or network.

29.2 Computers may not be "booted" from an external portable media device received from an outside source and all portable media devices must be removed from a computer when not in use.

29.3 Employees may not store personal information on portable media devices.

29.4 Employees must report loss of portable devices to the Information Officer.

29.5 When an Employee leaves the employ of Get SACE Points, all portable media devices in their possession must be returned to the Information Officer.

29.6 Employees must ensure that portable media devices are wiped clean of all data if no longer in use. All external media must be sent to Get SACE Points' IT personnel to ensure the correct processes are followed.

30 MOBILE DEVICES

30.1 Employees occasionally have access to email and other work-related applications on their personal mobile devices. Employees must obtain prior approval from Get SACE Points' IT personnel in order to access email on their mobile devices.

30.2 Get SACE Points shall keep a register in order to record which Employees have access to email or work-related applications on their mobile devices and to ensure that such access is revoked when the Employee leaves the employ of Get SACE Points.

30.3 Employees must make use of two-factor authentication in order to access emails from a mobile device and such mobile device must have adequate protection from use of third parties in the form of passwords or fingerprint/facial recognition.

31 PROHIBITED ACTIVITIES

Employees may not -

31.1 deliberately crash an information system. If a crash occurred because of user action, a repetition of the action by the Employee may be viewed as a deliberate act;

31.2 attempt to break into an information resource or to bypass a security feature;

31.3 introduce, or attempt to introduce, computer viruses, trojan horses, peer-to-peer or other malicious code into an information system unless specifically authorised

in writing by the Information Officer for the purpose of testing hardware or software by IT personnel;

31.4 wilfully access or inspect confidential or sensitive information which is not authorised or approved on a "need to know" basis;

31.5 use or install personal software on Get SACE Points computers;

31.6 violate or attempt to violate the terms of use or license agreement of any software product used by Get SACE Points;

31.7 engage in any activity for any purpose that is unlawful or contrary to the policies, procedures, or business interests of Get SACE Points; or

31.8 use resources provided by Get SACE Points, such as individual computer workstations or laptops, computer systems, networks, e-mail, and internet software and services ("**Resources**") for any purpose other than for the business of Get SACE Points and for incidental personal use as set out in 32.

32 INCIDENTAL PERSONAL USE

Incidental personal use of Resources is permissible only if -

32.1 it does not interfere with Employee productivity; and

32.2 it does not pre-empt any business activity.

33 VIOLATIONS

The Resources may not be used -

33.1 to perform copyright violations, including the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright;

33.2 for or in support of illegal activities;

33.3 for personal or commercial profit;

33.4 to conduct political activities;

33.5 to disrupt, offend, or harm any person including by -

33.5.1 the display or transmission of sexually explicit images, messages, or cartoons;

33.5.2 the display or transmission of ethnic slurs, racial comments, or off-colour jokes; or

33.5.3 anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening, or showing disrespect for others; or

33.6 to distribute “junk” mail, such as -

33.6.1 chain letters (a letter sent to several persons with a request that each send copies of the letter to a number of persons);

33.6.2 advertisements; or

33.6.3 unauthorised solicitations.

34 MONITORING

34.1 Generally, while it is not the policy of Get SACE Points to monitor the content of any electronic communication, Get SACE Points is responsible for servicing and protecting its equipment, networks, data, and Resources and therefore may be required to access and/or monitor electronic communications of Employees from time to time.

34.2 Get SACE Points reserves the right, at its discretion, to review any Employee’s files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations, this Policy and any other policies of Get SACE Points issued from time to time.

34.3 Employees should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed, or stored by others.

PART VI – SECURITY MEASURES

This Part VI sets out the general security policy of Get SACE Points and measures implemented in order to protect the personal information, specifically in respect of information technology measures.

35 SECURITY POLICY

35.1 Get SACE Points takes appropriate, reasonable technical and organisational measures to prevent –

35.1.1 loss of, damage or unauthorised destruction of personal information; and

35.1.2 unlawful access to or processing of personal information.

35.2 In this regard Get SACE Points –

35.2.1 employs data security technology to secure the personal information and protect it against threats;

35.2.2 has implemented information technology security measures to support the objects of this Policy;

35.2.3 limits access to personal information to those Employees who require access for the purpose of performing their obligations; and

35.2.4 requires Employees to sign confidentiality agreements or employment agreements which include confidentiality undertakings.

35.3 Each Employee must comply with the safety and security measures of Get SACE Points when processing personal information.

35.4 Get SACE Points will continuously review its security controls and processes to ensure that all personal information is secure.

35.5 <u>Virus Protection</u>

35.5.1 Employees may not stop the update process for virus protection as it is critical to the security of all data and must be allowed to complete. Virus protection software must be installed on all the company computers.

35.5.2 Should an Employee disable a virus scanner or firewall, it will be viewed in a serious light and may lead to disciplinary procedures being instituted against the Employee.

35.6 Personal Computers

Employees may be authorised to use their personal computers for work purposes provided that -

35.6.1 it has been authorised in writing by the Information Officer;

35.6.2 Get SACE Points' IT personnel have set up a separate profile to divide use of the computer for work and for personal purposes;

35.6.3 approved virus protection software has been installed; and

35.6.4 VPN settings have been configured by Get SACE Points' IT personnel to ensure access to Get SACE Points' servers are secure.

36 IDENTIFICATION AND AUTHENTICATION

36.1 User Logon IDs

In order to access Get SACE Points computer workstations, laptops, and systems, or Get SACE Points profiles on personal computers, individual users must have unique logon IDs and passwords. Get SACE Points has implemented an access control system which identifies each user and prevents unauthorised users from entering or using information resources. Listed below are the security requirements for user identification -

36.1.1 Each user shall be assigned a unique identifier.

36.1.2 Users shall be responsible for the use and misuse of their individual user ID.

36.1.3 All user IDs on Get SACE Points' systems and are reviewed monthly and all inactive user IDs are revoked.

36.1.4 The logon ID is locked after a maximum of 3 unsuccessful logon attempts which then require the passwords to be reset.

36.2 Passwords

Along with the user IDs, passwords are required to gain access to Get SACE Points' systems. All passwords are restricted by a corporate-wide password policy to be of a "strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

37 NETWORK CONNECTIVITY

37.1 VPN Connections

Access to Get SACE Points' networks shall be subject to authorisation and authentication by an access control system.

37.2 Connections to External Networks / Computers

As connecting to external networks or computers result in a higher security risk, IT personnel will ensure that the correct infrastructure is in place and that all security protocols are followed where Get SACE Points computers or laptops are connected to external networks, or where an external computer is used to connect to Get SACE Points' network or systems.

38 MALICIOUS CODE

38.1 Get SACE Points will maintain a record of virus patterns for all computers and servers on Get SACE Points network. Appropriate IT personnel are responsible for providing reports for emergency situations, as requested by Get SACE Points.

38.2 Prior to the installation of any new software on Get SACE Points computers or networks, the software will be tested by appropriate IT personnel to ensure compatibility with currently installed software and network configuration. In addition, IT personnel must scan all software for viruses before installation.

PART VII – OFF-SITE PROCESSING

Get SACE Points recognises that telecommuting and working from home can be an advantage for Employees and for Get SACE Points in general, but that it presents new risks in the areas of confidentiality and security of data. Employees linked to Get SACE Points network become an extension of the wide area network and present additional environments that must be protected against the danger of spreading trojans, viruses, or other malware.

This Part VII accordingly sets out the processes and rules to be followed where personal information is processed outside of Get SACE Points' offices, specifically for purposes of working from home.

39 OFF-SITE PROCESSING AND DATA SECURITY

39.1 The following provisions are applicable to all Employees who work outside of the office environment, including Employees -

39.1.1 who work from their home full time;

39.1.2 on temporary travel;

39.1.3 who work from a remote office location; and

39.1.4 to any Employee or other party who connects to Get SACE Points' network from a remote location.

39.2 Devices

All devices used for off-site processing must be approved by the Information Officer in writing. Get SACE Points shall keep a register to record all approved devices. Employees are not to work on their personal devices unless otherwise authorised by the Information Officer in writing.

39.3 Passwords

The use of a strong password is even more critical when working off-site. Employees may not share their password or write it down where a family member, visitor or third party can see it.

39.4 Transferring Data to Get SACE Points

Transferring of data to Get SACE Points requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Employees may not circumvent established procedures, nor create their own methods when transferring data to Get SACE Points.

39.5 Viewing Personal Information in a Public Location

Employees must not perform work tasks which require the use of personal information when they are in a public area, i.e., airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind an Employee.

PART VIII – SECURITY COMPROMISES

This Part VIII outlines the contingency plan and sets out the procedure to be followed in the event of a security compromise, including notification requirements.

40 CONTINGENCY PLAN

40.1 Get SACE Points is committed to maintaining formal processes for responding to an emergency or other occurrence that damages systems containing personal information. Get SACE Points shall continually assess potential risks and vulnerabilities to protect information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures.

40.2 The IT personnel shall monitor storage and removal of backups and ensure all applicable access controls are enforced.

40.3 All company servers shall be backed up daily and server backups shall be kept for 30 days and shall be stored in a secure access-controlled data centre.

40.4 Backup procedures shall be tested monthly to ensure that exact copies of information can be retrieved and made available. Such testing shall be documented by IT personnel. To the extent such testing indicates need for improvement in backup procedures; the IT personnel shall identify and implement such improvements in a timely manner.

40.5 Disaster Recovery Plan

40.5.1 The IT personnel shall be responsible for developing and regularly updating the written disaster recovery plan for the purpose of -

40.5.1.1 restoring or recovering any loss of information and/or systems necessary to make information available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and

40.5.1.2 continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall

be maintained on-site and at the off-site locations at which backups are stored.

40.5.2 The disaster recovery plan shall include the following -

40.5.2.1 A current copy of the written backup procedures developed and updated pursuant to this policy.

40.5.2.2 The members of an emergency response team, which team shall be responsible for the following -

40.5.2.2.1 determining the impact of a disaster and/or system unavailability on Get SACE Points' operations;

40.5.2.2.2 securing the site and providing on-going security;

40.5.2.2.3 retrieving lost data;

40.5.2.2.4 identifying and implementing appropriate "work-arounds" during such time information systems are unavailable;

40.5.2.2.5 taking such steps necessary to restore operations;

40.5.2.2.6 telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following -

40.5.2.2.6.1 members of the immediate response team; and

40.5.2.2.6.2 facilities at which backup data is stored;

40.5.3 The disaster recovery team shall meet on at least an annual basis to -

40.5.3.1 review the effectiveness of the plan in responding to any disaster or emergency experienced by Get SACE Points; and

40.5.3.2 review the written disaster recovery plan and make appropriate changes to the plan.

40.5.4 Get SACE Points' IT personnel shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

41 REPORTING SOFTWARE MALFUNCTIONS

41.1 In the event that an Employee's software does not appear to be functioning correctly, the Employee should inform the appropriate IT personnel as the malfunction - whether accidental or deliberate - may pose a security risk.

41.2 If an Employee suspects a computer virus infection, the Employee must -

41.2.1 immediately stop using the computer;

41.2.2 not carry out any commands, including commands to 'save' data;

41.2.3 not close any of the computer's windows or programs;

41.2.4 not turn off the computer or peripheral devices;

41.2.5 if possible, physically disconnect the computer from networks to which it is attached;

41.2.6 inform the appropriate IT personnel as soon as possible;

41.2.7 write down any unusual behaviour of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed;

41.2.8 write down any changes in hardware, software, or software use that preceded the malfunction; and

41.2.9 not attempt to remove a suspected virus.

41.3 Get SACE Points' IT personnel should monitor the resolution of the malfunction or incident, and report to the result of the action with recommendations on action steps to the Information Officer to avert future similar occurrences.

42 REPORT SECURITY INCIDENTS

42.1 Employees are responsible for the day-to-day, hands-on security of Get SACE Points Resources that they use and must formally report all security incidents or violations of this Policy immediately to the Information Officer.

42.2 Reports of security incidents shall be escalated as quickly as possible. Each incident will be analysed to determine if changes in the existing security structure are necessary.

42.3 All reported security incidents shall be logged, and the remedial action indicated. It is the responsibility of Get SACE Points' IT personnel to provide training on any procedural changes that may be required because of the investigation of an incident.

43 INTERNAL BREACH NOTIFICATION PROCEDURES

43.1 Containing the Breach

In the event of a security breach, Get SACE Points' IT personnel shall take the steps listed below to limit the scope and effect of the breach.

43.1.1 Stopping the unauthorised practice.

43.1.2 Recovering the records, if possible.

43.1.3 Shutting down the system that was breached.

43.1.4 Mitigating the breach, if possible.

43.1.5 Correcting weaknesses in security procedures and systems.

43.2 Investigating the Breach

43.2.1 To determine what other steps are immediately necessary, Get SACE Points' IT personnel in collaboration with the affected department(s) and the Information Officer, will investigate the circumstances of the breach.

43.2.2 Get SACE Points' IT personnel will review the results of the investigation to determine root cause(s), evaluate risks, and develop a resolution plan.

43.3 Prevention

43.3.1 Once immediate steps are taken to mitigate the risks associated with the breach, Get SACE Points' IT personnel will investigate the cause thereof.

43.3.2 If the Information Officer determines that it is necessary, Get SACE Points will (in conjunction with IT personnel) conduct a full security audit of physical, organisational, and technological measures and review the mitigating steps taken.

43.3.3 Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.

44 EXTERNAL NOTIFICATION OF SECURITY COMPROMISE

44.1 Subject to clause 44.4, where there are reasonable grounds to believe that the personal information has been accessed by any unauthorised person, Get SACE Points will notify –

44.1.1 the Regulator;

44.1.2 the Subject affected by the security compromise unless the identity of the Subject cannot be established; and

44.1.3 the South African Police Service, in the event that criminal activity is suspected.

44.2 The notification must be made as soon as reasonably possible after the discovery of the compromise, considering the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the compromise and to restore the integrity of Get SACE Points' information system.

44.3 Get SACE Points will only delay notification as aforesaid if a public body responsible for the prevention, detection or investigation of offences or the Regulator determines that notification will impede a criminal investigation by the public body concerned.

44.4 The notification will be in writing and communicated to the applicable Subject by way of electronic mail or by such other means authorised in terms of the Act.

44.5 Any notification in terms of this clause 44 must be approved by the Information Officer in writing.

44.6 The notification must provide sufficient information to allow the Subject to take protective measures against the potential consequences of the compromise, including –

44.6.1 a description of the possible consequences of the security compromise;

44.6.2 a description of the measures that Get SACE Points intends to take or has taken to address the security compromise;

44.6.3 a recommendation with regard to the measures to be taken by the Subject to mitigate the possible adverse effects of the security compromise; and

44.6.4 if known to Get SACE Points, the identity of the unauthorised person who may have accessed or acquired the personal information.

PART IX – RESPONSIBILITIES AND COMPLIANCE

This Part IX sets out further information in respect of the Information Officer and his responsibilities and sets out the requirements for compliance with this Policy.

45 INFORMATION OFFICER

45.1 The Information Officer of Get SACE Points shall be its chief executive officer or equivalent officer or any person duly authorised by that officer.

45.2 Details of the Information Officer must be submitted to the Regulator. Get SACE Points must notify its Employees of the appointment of its Information Officer. The name and contact details of the Information Officer will also be made available to the public.

45.3 The Information Officer is responsible for –

45.3.1 encouraging and ensuring Get SACE Points' compliance with the conditions for the lawful processing of personal information;

45.3.2 dealing with requests made to Get SACE Points pursuant to the Act;

45.3.3 working with the Regulator in relation to investigations conducted in terms of Chapter 6 of the Act;

45.3.4 otherwise ensuring compliance with the provisions of the Act; and

45.3.5 such other functions as may be prescribed.

45.4 Get SACE Points must designate such number of persons as deputy information officers as are necessary to render Get SACE Points as accessible as reasonably possible to Subjects.

45.5 The Information Officer may delegate a power or duty conferred or imposed by the Act to a deputy information officer.

45.6 Any delegation to a deputy information officer –

45.6.1 must be in writing;

45.6.2 does not prohibit the information officer from exercising the power concerned or performing the duty concerned himself; and

45.6.3 may at any time be withdrawn or amended in writing by that person.

45.7 Any right or privilege acquired, or any obligation or liability incurred, as a result of a decision in terms of a delegation is not affected by any subsequent withdrawal or amendment of that decision.

45.8 Get SACE Points has appointed an information officer who has been tasked with the primary responsibility for compliance with the Act. The information officer's details are as follows –

Name: Paige Davidson

Email Address: paige@getsacepoints.co.za

Contact Number: 021 200 8877 / 066 023 4467

45.9 Should the identity of the Information Officer change at any time, Get SACE Points shall notify all of its Employees, directors and Operators in writing.

45.10 All Get SACE Points Employees are under a duty to -

45.10.1 raise any concerns in respect of the processing of personal information with the Information Officer;

45.10.2 promptly pass on to the Information Officer all Subject access requests and requests from third parties for personal information;

45.10.3 report losses or unauthorised disclosures of personal information to the Information Officer as soon as such loss or disclosure has been noted; and

45.10.4 address any queries or concerns about this Policy and/or compliance with the Act with the Information officer.

46 RESPONSIBILITIES

46.1 The Information Officer shall assess the controls in place to protect the personal information on a regular basis and shall note any concerns, modifications

required, additional training which should be implemented and all other matters to the board of Get SACE Points for consideration and implementation.

46.2 The board of Get SACE Points, in consultation with the Information Officer shall be responsible for ensuring that Employees are aware of the need to adhere to this policy and report non-compliance herewith to the Information Officer.

46.3 Employees are responsible for adhering to this Policy. Where the Policy requirements are reliant on Employees taking steps to secure the information they are handling, the individual Employee will be personally accountable for failing to follow the required procedure or process and may be subject to disciplinary proceedings. Employees must ensure that any risk of which they become aware of any breach of Get SACE Points' security systems is immediately reported to the Information Officer.

46.4 Third parties that are handling Get SACE Points' information, shall apply controls equivalent to those applicable to Get SACE Points' managed devices. These responsibilities, and Get SACE Points' right to audit the controls in place, shall be defined in the contract with the third party, as set out in clause 16.

47 COMPLIANCE

A breach of this Policy, including -

47.1 negligent loss of personal information;

47.2 unauthorised disclosure of personal information; or

47.3 failure to report negligent loss or unauthorised disclosure of personal information,

shall be treated in a serious light, and the Employee may be subject to disciplinary proceedings dealt with under Get SACE Points' disciplinary policies as appropriate. Where third parties are involved breach of this policy may also constitute breach of contract.

48 ADOPTION AND AMENDMENT OF POLICY

48.1 This Policy is adopted with effect from 30 June 2021.

48.2 Get SACE Points shall notify all Employees of the contents of this Policy from which date they shall be responsible to comply with the provisions hereof insofar as they are applicable to such Employees.

48.3 Get SACE Points may amend, vary, replace, or supplement this Policy at any time, subject to written notice to all Employees.