DATA BREACH REPORTING POLICY

1. INTRODUCTION:

1.1. This Policy defines the steps that personnel must use to ensure that information security incidents are identified, contained, investigated, and remedied.

1.2 This policy further provides a process for documentation, appropriate reporting internally and externally, and communication so that organizational learning occurs.

1.3 The policy establishes responsibility and accountability for all steps in the process of addressing information security incidents.

1.4 The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities and standards. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

2. APPLICATION OF THE POLICY

2.1 This Policy applies to staff members who collects, processes, distribute and/or achives personal data, whether temporary or permanent staff, consultants, agents and contractors of the Company.

2.2 This Policy further applies to any computing or data storing devices owned or leased by the company that experience a Security Incident, as well as any computing or data storing device, regardless of ownership, which is used to store Protected Personal Data, or which, if lost, stolen, or compromised, and based on its privileged access, could lead to the unauthorized disclosure of Protected Personal Data

3. DEFENITIONS

3.1 “Data Breach” Any incident where data was obtain by a third party.

3.2 “Data Subject” Any person and/or entity whose information has been collected, processed, distributed and/or arched by the Company.

3.2 “Information Officer or IO” Allocated person within the organisation who oversees, monitor and ensures compliance with the relevant legislations. The IO is also responsible to investigate and report on data breaches.

3.3 "Personal Data" Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.
- Personal data may also include special categories of personal data or criminal conviction and offences data. These are considered to be more sensitive and you may only process them in more limited circumstances.
- Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data.
- If personal data can be truly anonymised, then the anonymised data is not subject to the POPIA. It is important to understand what personal data is in order to understand if the data has been anonymised.
- Information about a deceased person does not constitute personal data and therefore is not subject to the POPIA.
- Information about companies or public authorities is not personal data.
- However, information about individuals acting as sole traders, employees, partners and company directors where they are individually identifiable and the information relates to them as an individual may constitute personal data.

3.4 "Security Incident" Any incident that could have resulted or may possibly result in a data breach.

3.5 "User" Any person that uses the system and/or have access to the company systems for any whatsoever reason.

4. PROCEDURE

4.1 Identifying and Reporting Security Incidents

4.1.1 In the event that a User detects a suspected Security Breach, the User must report the Security Incident immediately to the IO. The User will be asked to provide the following information:

- User contact information
- Name(s) of department(s) involved

- A brief description of what happened
- A general description of the Protected Personal Data affected recommendations about the steps individuals should take in response to the data breach

As directed by the responsible person or IO, the reporter shall follow instructions regarding securing data and preserving evidence.

4.2 **Security Incident Protocol**

4.2.1 The IO will notify the relevant department of the Security Incident, log the incident, and initiate evaluation.

4.2.2 The evaluation process shall include:

- Securing the Data,
- Preserving evidence,
- Contacting Law Enforcement, if appropriate, and
- Establishing the scope of the Incident.

4.2.3 Once the IO has completed the initial evaluation, the IO shall communicate the results to the relevant Departmental Manager.

4.2.4 The IO in coordination with the relevant Departmental Manager will make a determination regarding whether a Security Breach has occurred and the type of Personal Data involved.

4.3 **Steps to be taken in the event of a Security breach**

4.3.1 The IO will brief the relevant departments whose data have been compromised by the breach.

4.3.2. The IO will advise the department on where and/or how the breach occurred, the data that has been compromised, and the data subjects that have been affected by the incident.

4.3.3 The Departmental Manager that was responsible for maintaining the breached information will be required, in consultation with the IO, for notifying the affected individuals or business associates of the security incident.

4.3.4 The IO, in consultation with the Departmental Manager, shall notify the Information Regulator, as required, of the breach.

4.3.5 The DPO will make recommendations to the department(s) to correct or improve information security practices that may have led to the incident.

4.4 If it is determined a security breach did not occur;

4.4.1 The IO will, when appropriate, make remedial suggestions to the User and/or department(s) to correct or improve information security practices that may have led to the incident.

5. NOTICE REQUIREMENTS

5.1 In the event of a security breach affected individuals shall receive a notice of the incident, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or the Information Regulator.

5.2 The method of reporting and/or information data subjects of a breach may vary dependent on the number of individuals affected, the cost of notifying the relevant parties, and the normal means of communication with affected individuals, but in all instances as guided by the applicable legal requirements.

5.3 The company may outsource some or all of the breach notification requirements depending on the nature and extent of the breach.

5.4 The data subjects is, however, required to be informed in writing which may include, emails, SMS's, post.

5.6 Documentation of the Incident and/or breach

5.6.1 The Company will document all reported information of the security breach including; the evaluation process and outcome of the evaluation and recommended corrective action to contain the incident and prevent future incidents, breach determination outcome, identification of Responsible party, and documentation of notice made to affected individuals, or authorities, where applicable.

5.7 Notice Requirements

5.7.1 The IO should be informed of the security breach as soon as it is discovered.

5.7.2 The data subjects should be informed of the breach as soon as possible and without unreasonable delay after the discovery or notification, consistent with the relevant authorities' needs, or with any measures necessary to determine

the scope of the security breach and restore the reasonable integrity, security, and confidentiality of the data system.

5.8 **Content of the Notice**

5.8.1 The content included in the notice shall be clear and conspicuous and include a description of each of the following, if known:

- Communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- Describe the likely consequences of the personal data breach;
- Describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects;
- The incident in general terms;
- The type and nature of Personal data breach including where possible:
    1. The categories and approximate number of data subjects concerned, and
    2. The categories and approximate number of personal data records concerned;

- The general acts of the data collector to protect the Personal Data from further breach;
- Describe the likely consequences of the personal data breach;
- A telephone number or email address, that the individual may call for further information and assistance;
- Advice that directs the individual to remain vigilant by reviewing account statements and monitoring free credit reports where applicable;
- The approximate date of the breach; and
- A description of the measures taken or proposed to be taken by the Information Officer to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.9 **Methods of Notice:**

5.9.1 Data Subjects may be informed of the security breach in one of the following manners;

- Written notice mailed to the data subject's residential/postal/ commercial address;
- Electronic notice, for those data subjects for whom the Company has a valid e-mail address if the Company does not have contact information.

5,9.2 The Notice to the data subject must:

- Use clear and plain language
- Describe the nature of the personal data breach
- Contain at least the following information

1. The name and contact details of the data protection officer or other contact point where more information can be obtained;
2. The likely consequences of the personal data breach;
3. The measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

6. DETAILS OF THE INFORMATION OFFICER

6.1 Questions related to the daily operational interpretation of this policy or any security breaches should be directed to the Information Officer: Andrew Miskell

7. BREACH DUE TO NEGLIGENCE

Any employee that is found to be responsible for an event where a breach of information security occurs through negligence, or non-compliance to the Company's policy prescriptions, or any person that has knowledge of such an occurrence and fails to report the incident for whatever reason, will be held fully accountable for the incident and subjected to the Disciplinary Code procedures of the Company. The contractual agreements of external third party contractors to the Company will be subject to immediate suspension or termination in the sole discretion of the senior management of the Company.

8. PREVENTING FUTURE BREACHES

Once the data breach has been dealt with, the School will consider its security processes with the aim of preventing further breaches. In order to do this, we will: -

- Establish what security measures were in place when the breach occurred;
- Assess whether technical or organisational measures can be implemented to prevent the breach happening again;

- Consider whether there is adequate staff awareness of security issues and look to fill any gaps through training or tailored advice;
- Consider whether its necessary to conduct a privacy or data protection impact assessment;
- Consider whether further audits or data protection steps need to be taken;
- To update the data breach register;
- To debrief governors/management following the investigation.

9. MONITORING AND REVIEW

We will monitor the effectiveness of this and all of our policies and procedures and conduct a full review and update as appropriate. Our monitoring and review will include looking at how our policies and procedures are working in practice to reduce the risks posed to the Company.

The Company will review and learn from the data breach to improve its personal data handling practices and prevent the recurrence of similar data breaches.

This may involve:

1. review including a root cause analysis of the data breach (e.g., implement fixes to system errors/bugs to prevent future disclosure of/access to personal data)
2. A prevention plan to prevent similar data breaches in future
3. Audits to ensure the prevention plan is implemented
4. A review of existing policies, procedures and changes to reflect the lessons learnt from the review
5. Changes to employee selection and training practices
6. A review of data intermediaries involved in the data breach