Reach Student Life Management

CYBERSECURITY INCIDENT RESPONSE PLAN

Prepared by: Touchline Connect Pty Ltd

Last Modified: 24/03/2021

TABLE OF CONTENTS

PURPOSE 2
DEFINITIONS 3
AFFECTED STAKEHOLDERS 4
REPORT MANAGEMENT 4
COMMUNICATION GUIDELINES 4
DATA BREACH RESPONSE TEAM 5

PURPOSE

REACH Boarding System stores information related to students, staff, and internal business operations, as well as manages and maintains technical infrastructure required to house and maintain this information.

This Cyber Security Incident Response Plan outlines the procedures that Touchline Connect Pty Ltd and its subsidiary regional operators uses to detect and respond to unauthorized access or disclosure of private information from systems utilised maintained or serviced as part of the REACH Boarding System product.

This plan defines the roles and responsibilities of various staff with respect to the identification, isolation and repair of data security breaches, outlines the timing, direction and general content of communications among affected stakeholders, and defines the different documents that will be required during various steps of the incident response.

Touchline Connect Pty Ltd and its subsidiary regional operators also implements practices which are intended to proactively reduce the risk of unauthorised access or disclosure, such as training staff with respect to legal compliance requirements, following appropriate physical security and environmental controls for technical infrastructure, and deploying digital security measures such as firewalls, malware detection and numerous other industry standard systems.

In the event of a cyber security incident, Touchline Connect Pty Ltd, its subsidiary regional operators and staff have been trained to expeditiously deal with the matter. All management and staff are trained to recognise anomalies in the systems they regularly utilise, and to report any such anomalies as soon as possible to the Incident Response Manager so this Cybersecurity Incident Response Plan can be implemented. Throughout the year the Incident Response Manager and relevant staff are kept up to date on the latest security threats and trained in modern techniques of incident remediation.

DEFINITIONS

Cybersecurity Incident

A Cybersecurity Incident is any event that threatens the confidentiality, integrity or availability of the information resources we support or utilize internally, especially sensitive information whose theft or loss may be harmful to individual students, our partners or our organization.

Data Protection Officer (DPO)

Data protection officers are responsible for overseeing the company's data protection strategy and its implementation to ensure compliance with GDPR requirements and the company's Personal Data Privacy Policy.

Incident Response Manager (IRM)

The IRM oversees all aspects of the Cyber Security Incident. The key focuses of the IRM will be to ensure proper implementation of the procedures outlined in the Cyber Security Incident Response Plan, to keep appropriate Incident Logs throughout the incident. The IRM acts as the key liaison for the IRE for details, status and outcomes of the incident investigation. At the conclusion of a Cyber Security Incident, the IRM will conduct a review of the incident and produce both an Incident Summary Report and, where determined appropriate, a Process Improvement Plan.

Incident Response Executive (IRE)

The IRE oversees all aspects of the company's communications with stakeholders and affected parties. The key focuses of the IRE will be to monitor that the procedures outlined in the Cyber Security Incident Response Plan are being implemented and to act as the key liaison between the IRM, company management executives and other stakeholders such as clients or individuals.

Cyber Security Incident Log

The Cyber Security Incident Log will capture critical information about a Cyber Security Incident and the organizations response to that incident, and should be maintained while the incident is in progress.

Incident Summary Report (ISR)

The ISR is a document prepared by the IRM at the conclusion of a Cyber Security Incident and will provide a detailed summary of the incident, including how and why it may have occurred, estimated data loss, affected parties, and impacted services. Finally, it will examine the procedures of the Cyber Security Incident Response Plan, including the procedures when investigating the incident and whether updates are required. The template for the ISR may be seen in Appendix A.

Process Improvement Plan (PIP)

The PIP is a document prepared by the IRM at the conclusion of a Cyber Security Incident if the investigation and ISR provides recommendations for avoiding or minimizing the impact of future Cyber Security Incidents based upon the "lessons learned" from the recently-completed incident. This plan should be kept confidential for security purposes. The template for the PIP may be viewed in Appendix B

AFFECTED STAKEHOLDERS

In the event the incident involves the unauthorized access or disclosure of confidential student, staff, parent or other contacts the IRE or DPO will communicate information relevant to the incident as well as any additional requested information to which they have a right (e.g. specific student records, staff records, etc.). Touchline Connect Pty Ltd and its subsidiary regional operators does reserve the right to withhold certain information at the discretion of the IRM or DPO if that information may jeopardize current or future investigations, or pose a security risk to Touchline Connect Pty Ltd and its subsidiary regional operators or other entities or individuals.

In the event the incident is limited to REACH Boarding Systems not containing sensitive or confidential information, it will be the discretion of Touchline Connect Pty Ltd and its subsidiary regional operators and the IRM whether or not to share information related to the incident with outside stakeholders.

REPORT MANAGEMENT

All reports generated during an investigation along with any evidence gathered will be stored and managed by the IRM. Any physical records will be stored safely and securely by the IRE. Any digital records will be stored on the secure cloud network of Touchline Connect Pty Ltd.

COMMUNICATION GUIDELINES

- Initial communication to affected stakeholders should occur as expeditiously as possible upon the identification of the incident and in accordance with any legislated requirements for GDPR or other regional jurisdictions relating to personal data regulation.
- Communication with students, parents, staff or community members, will not be undertaken without first communicating with the school administration or representatives to ensure that;
  - The school is formally notified of any data breach, potential data breach or security incident, and
  - The school can approve any communication that is being provided to the students, parents, staff or community members related to their REACH Boarding System instance.
- In some cases, this may include an initial communication (letter, email, phone call) that simply ensures that the school is aware of the issue and that Touchline Connect Pty Ltd and its subsidiary regional operators is addressing it.

Personally Identifiable Information

Where a data breach or security incident occurs which may involve the compromise of Personally Identifiable Information (PII) the following communication guidelines apply:

- Should the unauthorized release of student or parent data occur, the Touchline Connect Pty Ltd and its subsidiary regional operators shall notify the school first and then the parents (or eligible students) affected by the release in the most expedient way possible.
- Should the unauthorized release of protected staff data occur, the district shall notify the school first and then the staff members affected by the release in the most expedient way possible.
- Updated communications will come from the IRE or from the IRM. If support staff at Touchline Connect Pty Ltd and its subsidiary regional operators receive requests from schools or individuals for information, they should pass those requests along to the IRE.

DATA BREACH RESPONSE TEAM

INCIDENT RESPONSE MANAGER (IRM)	
Mr Bradley Gibby *Director of Technology, Research & Development* *Touchline Connect Pty Ltd*	All regions Globally

INCIDENT RESPONSE EXECUTIVES (IRE)	
Mr Garry Jowett *Managing Director – Touchline Connect Pty Ltd*	Australia, New Zealand, Asia-Pacific, Africa, Rest of world
Mr Brian Murray *Managing Director – REACH North America*	USA, Canada
Mr Adam Bates *Managing Director – REACH Europe*	UK, Ireland, European Union

DATA PROTECTION OFFICERS (DPO)	
Mr Garry Jowett *Managing Director – Touchline Connect Pty Ltd*	Australia, New Zealand, Asia-Pacific, Africa, Rest of world
Mr Brian Murray *Managing Director – REACH North America*	USA, Canada
Mr James England *Director – REACH Europe*	UK, Ireland, European Union, GDPR designated DPO

ADDITIONAL MEMBERS
In addition to those individuals listed above, additional experts may be included on the Incident Response Team, depending upon the nature and scope of the incident. In particular, technical experts may be included from various providers of hardware or service services use by REACH Boarding System (such as cloud hosting service provider).