Miramar Rangers AFC
Privacy Breach

Miramar Rangers AFC ('Club') takes all measures and steps to ensure that the privacy of all of our members, including (but not limited to):

- The management committee
- Grade coordinators
- Coaches
- Managers
- Volunteers
- Players

If you believe a privacy breach has occurred, you should immediately contact the Club President (see contacts page at www.miramar-rangers.com for current Miramar Rangers AFC President). Details of the alleged privacy breach should be provided to the President in writing.

Once the President receives this information, the following procedure will be used in resolving the breach.

Privacy Breach Checklist

Incident Description

Include

1. Date of the incident?
2. When the incident was discovered?
3. How the incident was discovered?
4. Location of the incident?
5. Cause of the incident?

Step 1: Breach Containment and Preliminary Assessment

1.1 Contain the breach (computer system shut down, locks changed recovery of information).
1.2 Designate an appropriate individual to lead the initial investigation
1.3 Assemble a breach response team if required.to manage communications, risk management, legal. This may include specific members of the committee or any other person with appropriate skills.
1.4 Determine who needs to be made aware of the incident internally and potentially externally at this preliminary stage.
1.5 Determine whether the breach appears to involve theft or other criminal activity. If so, notify, the police. 1.6 Ensure that any evidence that may be necessary to investigate the breach is preserved.

Step 2: Evaluate the Risks Associated with the Breach

2.1 IDENTIFY ANY PERSONAL INFORMATION INVOLVED.

- Name, address, unique identifiers, financial, or medical information.
- Form of information, for example, paper records, electronic database?
- Physical or technical security measures in place at the time of the incident, for example, locks, alarm systems, encryption, passwords.

2.2 DETERMINE THE CAUSE AND EXTENT OF THE BREACH.

Identify:

- The risk of ongoing breaches or further exposure of the information;
- Whether personal information can be used for fraudulent or other purposes;
- Whether the information lost or stolen. If it was stolen, consider whether the information was the target of the theft or not.
- If personal information been recovered; and
- Whether this is a systemic problem or an isolated incident.

2.3 IDENTIFY INDIVIDUALS AFFECTED BY THE BREACH.

- Establish who, and how many, individuals have been affected by the breach. For example, members, volunteers, employees, contractors, public, service providers, other organisations.

2.4 IDENTIFY ANY FORESEEABLE HARM FROM THE BREACH.

Consider:

- The harm to the individuals that could result from the breach. For example, security risk, identity theft, financial loss, loss of business or employment opportunities, physical harm, significant humiliation or loss of dignity, or damage to reputation or relationships;
- who has received the information and the risk of further access, use or disclosure;
- any harm to the 'Club "that could result from the breach, for example, loss of trust, loss of assets, financial exposure, legal proceedings; and
- any harm that could come to the public as a result of notification of the breach, for example, risk to public health or risk to public safety.

Step 3: Notification

Notification can be an important mitigation strategy that has the potential to benefit both the agency and the individuals affected by the breach. If a privacy breach creates a risk of harm to the individual, those affected should be notified. Prompt notification to individuals in these cases can help them mitigate the damage by taking steps to protect themselves.

The key consideration in deciding whether to notify affected individuals should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been inappropriately accessed, collected, used or disclosed. Agencies should also take into account the ability of the individual to take specific steps to mitigate any such harm. There may also be situations where the individual cannot take any steps to mitigate potential harm, but the privacy breach was so material as to warrant notification.

3.1 NOTIFYING AFFECTED INDIVIDUALS

- In deciding whether to notify, consider: The legal and contractual obligations;
- The risk of harm to the individual;
- The risk of identity theft or fraud (usually because of the type of information lost, such as an individual's name and address and date of birth);
- The risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment)?
- The risk of significant humiliation or loss of dignity, damage to the individual's reputation or relationships;
- The ability of the individual to avoid or mitigate possible harm.

If you decide that affected individuals do not need to be notified, record your reasons.

3.2 WHEN TO NOTIFY, HOW TO NOTIFY AND WHO SHOULD NOTIFY

Before notifying, ensure the breach and risk assessment have been completed.

When to notify:

Notification of individuals affected by the breach should occur as soon as reasonably possible following assessment and evaluation of the breach. However, if law enforcement authorities are involved, check with those authorities whether notification should be delayed to ensure that the investigation is not compromised.

How to notify:

The preferred method of notification is direct – by phone, letter, email or in person – to affected individuals.

Indirect notification – website information, posted notices, media – should generally only occur where direct notification could cause further harm, is prohibitive in cost or the contact information for affected individuals is not known. Using multiple methods of notification may be appropriate. Consider whether the method of notification might increase the risk of harm, for example, by alerting the person who stole the laptop to the value of the information on the computer.

Who should notify:

An appointed representative from the club e.g. Club President should notify the affected individuals, including when the breach occurs at a third party service provider that has been contracted to maintain or process the personal information unless notification by a third party is more appropriate.

3.3 WHAT SHOULD BE INCLUDED IN THIS NOTIFICATION?

Depending on the circumstances, notifications could include some of the following, but be careful to limit the amount of personal information disclosed in the notification to what is necessary:

- Information about the incident and its timing in general terms
- A description of the personal information involved in the breach
- A general account of what your agency has done to control or reduce the harm
- What the club will do to assist individuals and steps individuals can take to reduce the risk of harm or further protect themselves
- Sources of information designed to assist individuals in protecting against identity theft
- Contact information of a department or individual within the club who can answer questions or provide further information
- Whether the club has notified other agencies e.g. NZ Police, the Office of the Privacy Commissioner, Capital Football

Additional contact information for the individual to address any privacy concerns to the club.1

3.4 Should the Office of the Privacy Commissioner be informed? www.privacy.org.nz/contact-us/

- Should the NZ Police or any other parties be informed? This may include insurers; professional or other regulatory bodies; credit card companies, financial institutions or credit reporting agencies; other internal or external parties such as third party contractors, internal business units not previously advised of the privacy breach, union or other employee representatives)?

3.5 OTHERS TO CONTACT

Office of the Privacy Commissioner: For further information refer to http://privacy.org.nz/privacy-breach-guidelines-2/?highlight=Privacy breach

Police: if theft or other crime is suspected.

Insurers or others: if required by contractual obligations.

Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies.

Credit card companies, financial institutions or credit reporting agencies: if their assistance is necessary for contacting individuals or assisting with mitigating harm.

Other internal or external parties not already notified:

- Third party contractors or other parties who may be affected

Step 4: Prevention of Future Breaches

- Identify the short or long-term steps required to correct the situation, for example, staff training, policy review or development, audit.