Key Steps for Clubs in Responding to Privacy Breaches

Purpose

The purpose of this document is to provide guidance to clubs on what steps to take if a privacy breach occurs. Clubs should take preventative steps prior to a breach occurring by having reasonable policies and procedural safeguards in place, and conducting necessary staff/ volunteer training. These guidance documents are intended to help clubs take the appropriate steps in the event of a privacy breach and to provide guidance in assessing whether notification to affected individuals is required. Not all steps may be necessary, or some steps may be combined.

The guidance material is also intended to assist clubs to plan in advance for a breach to ensure that they are prepared to manage it successfully for the benefit of the club and affected individuals.

What is a privacy breach?

A privacy breach occurs when there is unauthorised access to or collection, use, or disclosure of personal information. Such activity is "unauthorised" if it occurs in contravention of the Privacy Act 1993 (or applicable code of practice issued under the Act). Some of the most common privacy breaches happen when personal information of members, or employees/ volunteers is stolen, lost or mistakenly disclosed (e.g. a computer containing personal information is stolen or personal information is mistakenly emailed to the wrong people). A privacy breach may also be a consequence of faulty organisational procedure or an operational break-down.

Four key steps in responding to a privacy breach

There are four key steps to consider when responding to a breach or suspected breach:

1) Breach containment and preliminary assessment;
2) Evaluation of the risks associated with the breach;
3) Notification; and
4) Prevention.

Be sure to take each situation seriously and move immediately to investigate the potential breach. Steps 1, 2 and 3 should be undertaken either simultaneously or in quick succession. Step 4 provides recommendations for longer-term solutions and prevention strategies. The decision on how to respond should be made on a case-by-case basis.

Attached to this document is a checklist that clubs can use to help ensure they have considered all the relevant factors when managing a possible privacy breach.

Step 1: Breach Containment and Preliminary Assessment

Once you have discovered, or suspect, that a privacy breach has occurred, you should take immediate common sense steps to limit the breach such as:

1.1 Immediately contain the breach. For example, stop the unauthorised practice, recover the records, shut down the system that was breached, revoke or change computer access codes or correct weaknesses in physical or electronic security.

1.2 Designate an appropriate individual to lead the initial investigation. This individual should be in a position within the organisation to conduct the initial investigation and make initial recommendations. If necessary, a more detailed investigation may subsequently be required.

1.3 Determine the need to assemble a team that could include representatives from appropriate parts of the organisation. This may include internal or external subject matter experts, such as forensic IT analysts, or risk advisers.

1.4 Determine who needs to be made aware of the incident internally, and potentially externally, at this preliminary stage. Escalate internally as appropriate, including informing the person within your club responsible for privacy compliance (typically the privacy officer).

1.5 If the breach appears to involve theft or other criminal activity, notify the police.

1.6 Do not compromise your ability or the ability of the police to investigate the breach. Be careful not to destroy evidence that may be valuable in determining the cause or allow you to take appropriate corrective action.

Step 2: Evaluate the Risks Associated with the Breach

To determine what other steps are immediately necessary, you should assess the risks associated with the breach. Consider the following factors in assessing the risks:

2.1 CONSIDER WHAT PERSONAL INFORMATION WAS INVOLVED

- What personal information has been breached?
- How sensitive is the information? Generally, the more sensitive the information the higher the risk of harm to individuals. Some personal information is more sensitive than other information. For example, health information, government-issued pieces of identification such as driver licence numbers, and financial account details such as credit or debit card numbers that could be used in combination for identity theft. A combination of personal information is typically more sensitive than a single piece of personal information. However, sensitivity is just one consideration when assessing the risk.
- What is the context of the personal information involved?.
- Is the personal information adequately encrypted, anonymised, or otherwise inaccessible?

- How can the personal information be used? Can the information be used for fraudulent or otherwise harmful purposes? The combination of certain types of sensitive personal information along with name, address and date of birth suggest a higher risk due to the potential for identity theft.
- An assessment of the type of personal information involved will help you determine how to respond to the breach, who should be informed, including the regional Football Federation, and what form of notification to the individuals affected, if any, is appropriate. For example, if a laptop containing adequately encrypted information is stolen, quickly recovered and investigations show that the information was not tampered with, notification to individuals may not be necessary.

2.2 ESTABLISH THE CAUSE AND EXTENT OF THE BREACH

- To the extent possible, determine the cause of the breach.
- Is there a risk of ongoing breaches or further exposure of the information?
- What was the extent of the unauthorised access to or collection, use or disclosure of personal information, including the number and nature of likely recipients and the risk of further access, use or disclosure, including via mass media or on-line?
- Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft?
- Has the personal information been recovered?
- What steps have already been taken to mitigate the harm?
- Is this a systemic problem or an isolated incident?

2.3 CONSIDER WHO IS AFFECTED BY THE BREACH

- How many individuals' personal information was affected by the breach?
- Who is affected by the breach, for example, members, volunteers, the public, clients, service providers, employees, other organisations?

2.4 IDENTIFY WHETHER HARM COULD FORESEEABLY RESULT FROM THE BREACH

In assessing the possibility of foreseeable harm from the breach, consider the reasonable expectations of the individuals affected.

Who is the recipient of the information? Is there any relationship between the unauthorised recipients and the affected individual(s)? For example, was the disclosure to an unknown party or to a party suspected of being involved in criminal activity where there is a potential risk of misuse? Or, was the recipient a trusted, known entity or person(s) that would reasonably be expected to return the information without disclosing or using it?

- What harm to the individuals could result from the breach? Examples include:
  - security risk, for example, physical safety
  - identity theft
  - financial loss

- loss of business or employment opportunities, or
- significant humiliation or loss of dignity, damage to reputation or relationships.

- What harm to the club could result from the breach? Examples include:
  - loss of trust in the club
  - loss of assets
  - financial exposure, or
  - legal proceedings.

- What harm could come to the public as a result of notification of the breach? Harm that could result includes:
  - 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 club 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 challenge is to determine when notices should be provided. Each incident needs to be considered on a case-by-case basis to determine whether privacy breach notification is necessary. Clubs are also encouraged to inform the regional Football Federation of material privacy breaches so they are aware of the breach and can effectively handle any related enquiries or complaints.

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. Clubs 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.

If the affected individual is notified, consideration should be given to whether steps are required to address potential on-going breaches, or effects which may, for instance, require a note of the breach on the individuals records.

3.1 NOTIFYING AFFECTED INDIVIDUALS

Clubs should consider the following factors when deciding whether to notify:

- What are the legal and contractual obligations?
- What is the risk of harm to the individual?
- Is there a reasonable risk of identity theft or fraud (usually because of the type of information lost, such as an individual's name and address together with government-issued identification numbers or date of birth)?
- Is there a risk of physical harm (if the loss puts an individual at risk of physical harm, stalking or harassment)?
- Is there a risk of significant humiliation or loss of dignity, damage to the individual's reputation or relationships, for example, when the information lost includes medical or disciplinary records?
- What is the ability of the individual to avoid or mitigate possible harm?

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

At this stage you should have as complete a set of facts as possible and have completed your risk assessment in order to determine whether to notify individuals.

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 the NZ Police are involved, check 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. You should also 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:

Typically, the club that has a direct relationship with the member, volunteer or employee 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. However, there may be circumstances where notification by a third party is more appropriate.

3.3 WHAT SHOULD BE INCLUDED IN THE NOTIFICATION?

The content of notifications will vary depending on the particular breach and the method of notification chosen. Notifications should include, as appropriate:

- 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 the club has done to control or reduce the harm;
- What the club will do to assist individuals and what steps the individual can take to avoid or reduce the risk of harm or to further protect themselves.
- Sources of information designed to assist individuals in protecting against identity theft. Some useful online guidance can be found on the following websites:
  - N.Z. Police: www.police.govt.nz/safety/home-identity-crime.html
  - Ministry of Consumer Affairs: www.consumeraffairs.govt.nz/mediacentre/wordofadvice/2007/20070702.html
  - Neighbourhood Support NZ: www.ns.org.nz/15.html
  - Netsafe: http://netsafe.org.nz/fraud/fraud_identity.aspx

- Contact information of an individual within your club who can answer questions or provide further information;
- Additional contact information for the individual to address any privacy concerns to the club
- Contact information for the regional Football Federation.
- Be careful not to include unnecessary personal information in the notice to avoid possible further unauthorised disclosure.

3.4 OTHERS TO CONTACT

Football Federation:

Clubs are encouraged to report material privacy breaches to the regional Football Federation as this will help the Football Federation respond to inquiries made by the public and any complaints received. The Football Federation may also be able to provide advice or guidance to your club that may be helpful in responding to the breach. Notifying the Football Federation may enhance the public's understanding of the incident and confidence in your club. The following factors should be considered in deciding whether to report a breach to the regional Football Federation:

- Whether the personal information is subject to privacy legislation;

- The circumstances of the breach, including:
  - the information breached;
  - the number of people affected by the breach;
  - whether the individuals affected have been notified, and
  - whether there is a reasonable expectation that the Football Federation may receive complaints or enquiries about the breach;

- Whether the disclosed information could be used to commit identity theft; and

- Whether there is a reasonable chance of harm from the disclosure including non monetary losses.

Regardless of what you determine your obligations to be with respect to notifying individuals, you should consider whether the following authorities or organisations should also be informed of the breach, as long as such notifications would be in compliance with the Privacy Act 1993, and any other relevant legislation.

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;
- The club committee
- Player representatives.

Clubs should consider the potential impact that the breach and notification of affected individuals may have on third parties and take actions accordingly.

Step 4: Prevention of Future Breaches

Once the immediate steps are taken to mitigate the risks associated with the breach, clubs need to take the time to investigate the cause of the breach and consider whether to develop a prevention plan. The level of effort should reflect the significance of the breach, and whether it was a systemic breach or an isolated instance. This plan may include the following:

- A security audit of both physical and technical security;
- A review of policies and procedures and any changes to reflect the lessons learned from the investigation and regularly after that, for example security policies, record retention and collection policies;
- A review of volunteer/ employee training practices; and
- A review of service delivery partners, for example, dealers or retailers.

The resulting plan may include a requirement for an audit at the end of the process to ensure that the prevention plan has been fully implemented.

Privacy Breach Checklist

Incident Description

1. What was the date of the incident?
2. When was the incident discovered?
3. How was it discovered?
4. What was the location of the incident?
5. What was the cause of the incident?

Step 1: Breach Containment and Preliminary Assessment

1.1 Have you contained the breach (recovery of information, computer system shut down, locks changed)?

1.2 Have you designated an appropriate individual to lead the initial investigation?

1.3 Is there a need to assemble a breach response team? If so, who should be included, for example, specific members of the committee, communications, risk management, legal?

1.4 Have you determined who needs to be made aware of the incident internally and potentially externally at this preliminary stage?

1.5 Does the breach appear to involve theft or other criminal activity? If yes, have the police been notified?

1.6 Have you made sure that evidence that may be necessary to investigate the breach is preserved?

Step 2: Evaluate the Risks Associated with the Breach

2.1 WHAT PERSONAL INFORMATION WAS INVOLVED?

- What personal information was involved, for example, name, address, unique identifiers, financial, or medical information?
- What form was the information in, for example, paper records, electronic database?
- What physical or technical security measures were in place at the time of the incident, for example, locks, alarm systems, encryption, passwords?

2.2 WHAT WAS THE CAUSE AND EXTENT OF THE BREACH

- Is there a risk of ongoing breaches or further exposure of the information?
- Can the personal information be used for fraudulent or other purposes?
- Was the information lost or was it stolen? If it was stolen, can it be determined whether the information was the target of the theft or not?
- Has the personal information been recovered?
- Is this a systemic problem or an isolated incident?

2.3 HOW MANY INDIVIDUALS HAVE BEEN AFFECTED BY THE BREACH AND WHO ARE THEY?

- 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 IS THERE ANY FORESEEABLE HARM FROM THE BREACH?

- What harm to the individuals 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.
- Do you know who has received the information and what is the risk of further access, use or disclosure?
- What harm to the agency could result from the breach, for example, loss of trust, loss of assets, financial exposure, legal proceedings?
- What harm 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

3.1 SHOULD AFFECTED INDIVIDUALS BE NOTIFIED?

- What are the reasonable expectations of the individuals concerned?
- What is the risk of harm to the individual? Is there a reasonable risk of identity theft or fraud?
- Is there a risk of physical harm? Is there a risk of humiliation or damage to the individual's reputation?
- What is the ability of the individual to avoid or mitigate possible harm?
- What are the legal and contractual obligations of the agency?

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

3.2 IF AFFECTED INDIVIDUALS ARE TO BE NOTIFIED, WHEN, HOW AND WHO WILL NOTIFY THEM?

- What form of notification will you use? For example, phone, letter, email or in person, website, media.
- Who will notify the affected individuals? Do you need to involve another party?
- If the NZ Police are involved, does notification need to be delayed to ensure that the investigation is not compromised?

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 your 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 your organization who can answer questions or provide further information
- Whether your club has notified the regional Football Federation
- Additional contact information to address any privacy concerns to your club, and
- Contact information for the regional Football Federation.

3.4 ARE THERE OTHERS WHO SHOULD BE INFORMED ABOUT THE BREACH?

- 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)?

Step 4: Prevention of Future Breaches

- What short or long-term steps do you need to take to correct the situation, for example, staff training, policy review or development, audit?