# Appendix E

## Breach of Private Information Procedure

**PURPOSE**

The purpose of this protocol is to outline the steps that must be followed in the event a breach of personal privacy is identified or suspected in the use of a payment card.

**PROCEDURE**

When a possible privacy breach has occurred, immediate action should be taken. The following procedure will assist in controlling the situation and ensuring that steps will be taken to minimize the risks of a similar breach from happening again.

**Step 1) Confirm and Contain.**

Confirm the validity of the suspected information breach. If the breach can be reasonably ascertained, containment should occur immediately. Containment includes, but is not limited to, disconnection of the host (e.g., server or other device) from the network or shutting down an application.

Care should be taken not to destroy data, but to preserve it without any form of network connection. Reconnection of the device to the network is not allowed until such time as remedial steps have been completed and re-connection is specifically approved by the Network Operations team or LAUSD’s Chief Information Security Officer.

**Step 2) Report.**

The following individuals are required to be informed as soon as possible:

1. LAUSD’s Chief Information Officer
2. The Chief Officer in the chain-of-command for the affected area.
3. The Office of General Counsel

The report, which will be coordinated by the Accounting and Disbursement Division’s General Accounting and Reporting Director, will indicate where possible whose personal information was disclosed, to whom it was disclosed, when it was disclosed, how it was disclosed/accessed, and what steps have been taken in response to the disclosure.

**Step 3a) Retrieve.**

Any documents or contents of electronic documents that have been disclosed to, or taken by, an unauthorized recipient should immediately be retrieved and secured (electronic documents or paper documents in facsimile form or printed email messages) or taken offline.

Documents, in any form, should not be destroyed until specific instruction is received. This may require personal attention to secure the documents and return them to their original location, remove them permanently from electronic storage or send them to the intended authorized recipient.

**Step 3b) Remove.**

Private information taken offline (Step 1 and Step 3a) may still be accessible and discoverable on the Internet via Internet Search engines (e.g., Google). The usual time periods for information to be removed by the search engines through routine web crawling techniques is too elongated (e.g., weeks) and requests must be made to remove the information from search engine indexes and cache directly to the Internet Search engines companies. These requests must be made as quickly as possible. However, removal of data should not occur without the involvement of OGC and or the Los Angeles School Police Department, as it could be evidence in an investigation.

Support request procedures for the major search engines at the time of this document’s creation are available as links below. This step, if necessary, will be coordinated under the direction of the Chief Information Security Officer.

Internet Search Engines: Clearing the index and Cache

* Google: <http://www.google.com/intl/en/webmasters/remove.html>
* Internet Search Engines: <http://searchenginewatch.com/>
* Bing: <https://www.bing.com/webmaster/help/bing-content-removal-tool-cb6c294d>
* UC Berkeley, The Best Search Engines: <http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/SearchEngines.html>
* The Wayback Machine, Internet Archive: <http://www.archive.org/about/faqs.php#2>
* Yahoo: <https://help.yahoo.com/kb/search/SLN2214.html?impressions=true>

**Step 4) Notify.**

In cases where the breach results in the disclosure of personal information, California law may require that the affected individual(s) be notified.

Determination of reporting requirements will be made by the Office of the General Counsel on a case-by-case basis. The notification message and timing will be handled by the Office of the General Counsel exclusively – all personnel that are aware of a breach or that may be working on matters related to a breach must direct all communication regarding a breach back to the Office of the General Counsel.

LAUSD will follow the guidance on Notification and Communication as outlined by the Federal Trade Commission:

<https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/volumeii.pdf>

and California’s Reporting Requirements for a Security Breach Involving Personal Information:

<https://oag.ca.gov/privacy/databreach/reporting>

**Step 5) Investigate.**

LAUSD’s Office of the General Counsel, the Chief Information Officer, and the Network Operations department will coordinate the investigation of any breach, for the purpose of determining and recording all the relevant facts concerning the breach and making recommendations. The objectives of this investigation include:

* a review of the circumstances surrounding the event as well as the adequacy of existing policies and procedures in protecting personal private information
* the impact of the breach and identification of all the individuals that were affected
* the actions that need to be taken to resolve immediate exposure, identification of vulnerabilities and steps to ensure future prevention

**Step 6) Management Review.**

The Office of General Counsel and Chief Information Officer will document and report the detail of the breach of privacy and remedial steps to the Superintendent of Schools.

**CONCLUSION**

A breach of private information is a serious matter. LAUSD staff and faculty and Central Office departments must make every reasonable effort to prevent breaches from occurring. If one does occur, staff and faculty must reference this policy and ensure that all procedures are followed.