Office of the
Privacy Commissioner
of Canada

STAPLES BUSINESS DEPOT

**Audit Report of the
Privacy Commissioner of Canada**

**Section 18 of the
*Personal Information Protection
and Electronic Documents Act***

FINAL REPORT

2011

Office of the Privacy Commissioner of Canada
112 Kent Street
Ottawa, Ontario
K1A 1H3

613-947-1698, 1-800-282-1376
Fax 613-947-6850
TDD 613-992-9190
Follow us on Twitter: @privacyprivee

© Minister of Public Works and Government Services Canada 2011

Cat. No. IP54-39/2011E-PDF
ISBN 978-1-100-18740-2

This publication is also available on our website at **www.priv.gc.ca**.

Table of Contents

Main Points

WHAT WE EXAMINED

During the period covering 2004–2008 the Office of the Privacy Commissioner (OPC) investigated two complaints wherein it was alleged that Staples Business Depot (Staples) failed to adequately protect personal information under its control. Both complaints related to the purchase and subsequent return of a data storage device. In both instances the devices were returned with personal information about the purchasers residing on them. Staples resold the devices without removing the data, which resulted in the improper disclosure of personal information to other customers. The complaints were resolved when Staples agreed to change some of its processes. In responding to the 2008 complaint, it agreed to implement a full "wipe-and-restore" procedure on all returned data storage devices. Subsequent to this there was a media report wherein it was alleged that another similar incident involving the company occurred. The circumstances surrounding the complaints and the subsequent media report were contributing factors in the Assistant Privacy Commissioner's determination that Staples had not implemented effective wipe-and-restore procedures to safeguard customer personal information, and that there may be ongoing contraventions of the *Personal Information Protection and Electronic Documents Act* (PIPEDA or the *Act*). On that basis, the Assistant Privacy Commissioner concluded that reasonable grounds existed to undertake an audit of Staples' personal information management practices.

We examined Staples policies, practices and processes for managing personal information, with particular emphasis on the management of returned products with data storage capabilities. We conducted inspections of selected retail outlets to assess the physical and IT security controls used to safeguard personal information. In addition, we looked at Staples' business processes and forms, as well as its privacy awareness training program. Finally, we tested returned data storage devices destined for resale to ascertain whether they were properly sanitized (i.e., wiped and restored).

WHY THIS ISSUE IS IMPORTANT

A significant number of desktop computers, laptops, portable hard disks, memory sticks and digital cameras are sold to Canadians annually. These devices have the capacity to retain vast amounts of data, including personal information. Records and images that were traditionally retained in file folders, desk drawers and cabinets are increasingly stored on personal computing and electronic devices.

Many retail organizations have adopted a "satisfaction guaranteed or money refunded" policy to support their business operations. Consumers may purchase an item, use it for a specified period and if dissatisfied, return it for a full refund. Moreover, computing and electronic devices are generally subject to a manufacturer's warranty, whereby a consumer may return a defective unit within an established period and receive a replacement. Some of these returned items are refurbished, repackaged and resold.

There is a risk that such items may be resold prior to being fully wiped, potentially exposing personal information about previous purchasers. The unauthorized disclosure of such information could have serious consequences for these individuals, including financial loss resulting from identity theft or fraud, humiliation and damage to the individuals' reputations.

Implementing policies, procedures and controls to ensure personal information is accorded appropriate protection is a critical component of sound privacy management. As an organization subject to PIPEDA, Staples has an obligation to implement technical, physical and organizational safeguards to protect the integrity and security of its customers' personal information—including data residing on products that are returned or brought in for repair.

WHAT WE FOUND

Staples has adopted, as company policy, the 10 privacy principles listed in Schedule 1 of the *Act*. These principles have been embedded into a suite of corporate policies and procedures. Accountability for compliance with the *Act* is well defined and communicated. Employees are mindful of the importance of protecting customer data, as well as their roles and responsibilities in this regard.

We found that Staples generally limits its collection of personal information to the minimum required for service delivery. However, customers are not always informed of the uses that will be made of their personal information, or the circumstances under which the information may be transferred to the United States for processing.

Staples offers an online copy/print service for commercial clients and the general public. A request order, with the material to be printed attached, is submitted electronically. These records are kept for one year to facilitate the processing of subsequent orders for the same material. While this may have merit in terms of meeting business client needs, retaining personal information—resumés and legal documents such as separation and custody agreements—on the basis that it may have some future use is not in keeping with sound privacy management or the limiting retention principle.

Staples' policy requires that all personal information be secured, either in a locked cabinet or room, when not in use. We noted significant weaknesses in this area. Delivery, transfer and special order forms were stored in unlocked filing cabinets, and we observed returned data storage devices on open shelves and left unattended at service counters. We also noted instances of customer order forms (that contained personal information) being discarded in waste-baskets or recycling bins.

Before our audit, in an effort to prevent another privacy breach, Staples revised its procedures for processing returned computing and electronic devices with data storage capabilities. These procedures, which include sound control mechanisms, are not consistently applied. In 15 of the 17 stores audited, we found devices that were resealed and verified as wiped when such was not the case, devices that were not verified by a manager prior to being restocked, or devices that were sent directly to a return to vendor bin without being wiped.

We tested 149 data storage devices that had undergone Staples' wipe-and-restore process and were packaged for resale. The sample included computers, laptops, USB hard drives and memory cards. We found that 54 of the 149 devices tested contained customer data (this is data introduced onto the device, intentionally or otherwise, by or for the customer). A number of these devices contained personal information, including government-issued identification numbers, financial statements, employment histories, medical information, email messages, personal correspondence and photographs. Consequently, the management of returned data storage devices has not been addressed.

Controlled access to an IT system and the data stored within represents a key safeguard in protecting privacy. It mitigates the risk of personal information being compromised by restricting access to those with a legitimate need. We found that user activity is not logged to determine whether access rights have been appropriately exercised. Without a means of monitoring system access, Staples cannot be assured, with a reasonable degree of certainty, that customer data is used and disclosed for legitimate purposes in all instances.

Compliance with security procedures and controls are assessed under Staples' internal audit program. However, the Organization was unable to provide records to demonstrate that its collection, retention

and disposal of personal information is subject to formal reviews. An ongoing monitoring strategy, including audits, would provide a means of mitigating privacy risks and provide a level of assurance that fair information practices are integrated in Staples' day-to-day operations.

Staples Business Depot has responded to the audit recommendations and with one exception, has stated that it is committed to exploring ways to address the recommendations. All of the Organization's responses appear in italics, and are included after each of the OPC's recommendations. Both the audit recommendations and the Organization's responses are also listed in Appendix A of this report.

Introduction

ABOUT THE AUDIT ENTITY

1. Staples Business Depot (Staples) is a large retailer of office supplies, office furniture, business machines and electronic data storage devices such as desktop computers, laptops, hard drives and portable memory devices. Staples advised it accepts a number of these electronic devices back from its customers when they are not satisfied with a product as per its return policy. It operates over 300 retail outlets across Canada, specializing in servicing small business and home office customers. All business activities are centrally coordinated by Staples Canada Inc.'s head office in Richmond Hill, Ontario.

2. In addition to its retail (sales) business line, Staples offers photocopying and print services. There is also the provision for self-service copying. Requests for copying and print services may be made in person or online. Each store also features a Technology Centre that offers computer repair services, software installations, as well as computer upgrades and enhancements. Further information about Staples is available on its website at www.staples.ca.

REASONABLE GROUNDS FOR AUDIT

3. Between 2004–2008, the Office of the Privacy Commissioner (OPC) investigated two complaints wherein it was alleged that Staples failed to adequately protect personal information under its control. Both complaints related to the purchase and subsequent return of an electronic device with data capture capabilities. In both instances the devices were returned with personal information about the purchaser residing on them. Staples resold the devices without erasing the data, which resulted in the improper disclosure of personal information to other customers.

4. This Office found that Staples had failed to adequately safeguard the complainants' personal information, which resulted in the unauthorized disclosures. The complaints were resolved when Staples agreed to implement corrective action. In responding to the 2008 complaint, it agreed to implement a full "wipe-and-restore" procedure on all returned data storage devices. Subsequent to this there was a media report wherein it was alleged that another similar incident involving the company occurred. The circumstances surrounding the complaints and the subsequent media report were contributing factors in the Assistant Privacy Commissioner's determination that Staples had not implemented effective wipe-and-restore procedures to safeguard customer personal information, and that there may be ongoing contraventions of the *Personal Information Protection and Electronic Documents Act* (PIPEDA or the *Act*). On that basis, the Assistant Privacy Commissioner concluded that reasonable grounds existed to undertake an audit of Staples' personal information management practices.

FOCUS OF THE AUDIT

5. The audit focused on Staples' management of personal information about its customers. The objective was to assess whether the Organization had implemented adequate controls to protect personal information—including personal information residing on returned data storage devices—and whether its policies, processes and practices for managing such information comply

with the 10 privacy principles listed in Schedule 1 of PIPEDA. The audit did not assess or compare Staples personal information management practices with any practices or standards that may be followed by other retailers.

6. The audit did not include a review of Staples' handling of personal information about its employees nor did we audit any of Staples' third party service providers. Further, while the examination included an assessment of IT safeguards, the audit was not designed to examine Staples' overarching IT security infrastructure. Information on the scope, criteria and approach can be found in the **About the Audit** section of this report.

Observations and Recommendations

PRIVACY LEADERSHIP AND ACCOUNTABILITY

7. Organizations subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA or the *Act*) are responsible for the personal information in their control. To ensure this responsibility is understood, organizations are required to establish clear accountability for privacy and compliance with PIPEDA obligations. Accordingly, we expected to find that Staples had:

   - designated an individual or individuals to oversee compliance with PIPEDA; and
   - implemented policies, procedures and practices to address the 10 privacy principles listed in Schedule 1 of the *Act*.

8. We examined Staples' privacy policies and procedures, records outlining responsibility for privacy and corporate training materials. We also reviewed Staples' privacy breach management protocol. Although we noted examples of positive privacy practices, we did identify opportunities for improvement.

Roles and responsibilities are clearly defined and understood

9. In order to meet the obligations established under PIPEDA, accountability for compliance with the *Act* must be well defined and communicated. Staff must be educated on corporate privacy policies, processes and practices, and possess a clear understanding of their roles and responsibilities in terms of ensuring these compliance mechanisms function as intended.

10. While Staples' privacy policy assigns general responsibility for the protection of personal information to all employees, the Chief Privacy Officer (CPO) at Staples is responsible for overall strategic direction and privacy compliance at the executive level. The CPO's responsibilities include:

    - ensuring staff are adequately trained and understand their privacy obligations;
    - identifying and mitigating privacy risks; and
    - monitoring compliance with PIPEDA.

11. Compliance with the requirements of PIPEDA depends largely on how well the provisions contained therein are understood by those handling personal information. Awareness and training are essential to achieve the *Act*'s objectives.

12. Staples indicated that employee privacy awareness is a core element of how it manages privacy. Various mechanisms are used to enhance awareness, with mandatory privacy and information management training being the key component. This training is provided electronically. Completion rates are monitored by Staples' Head Office and reported monthly to store managers. We examined the training module and associated reference materials. These emphasize the importance of protecting personal information, present an overview of the 10 privacy principles and provide guidance on the collection, use, disclosure and disposal of personal information.

13. The mandatory privacy awareness program is supplemented by general staff meetings. This provides a forum for Staples' Head Office to communicate privacy-related issues

to employees. By way of example, a national campaign was recently undertaken to ensure all employees were aware of corporate contacts regarding privacy-related matters.

14. In addition to reviewing program records, we interviewed staff within Staples' various business lines. Generally, we found that customer service associates, technicians and managers were aware of the importance of protecting personal information, as well as their roles and responsibilities in this regard.

Privacy policies and procedures provide framework to protect personal information

15. Organizations subject to PIPEDA are required to implement policies and procedures to address the10 privacy principles listed in Schedule 1 of the *Act*. We expected to find such policies and procedures in place, and structured with sufficient detail to facilitate an understanding of how Staples' manages personal information that is entrusted to it.

16. We reviewed its privacy, information management and retention policies and associated guidance documents. We also examined procedures related to Staples' returns, repairs and data back-up operations. When examined collectively, these documents provide a comprehensive framework for protecting personal information.

17. Staples has adopted, as company policy, the 10 privacy principles listed in Schedule 1 of the *Act* to manage personal information. These are referenced in its Privacy Policy, which is available on its website. The policy does not elaborate on the type of personal information Staples collects, how it is used, to whom and under what circumstances it is shared with third parties, or how it is protected. The policy is also silent on the transmission and storage of personal information outside Canada. By contrast, the above collection, use and disclosure practices are outlined in significant detail in Staples' U.S. Privacy Policy.

18. An organization's privacy policy is an essential tool in safeguarding customers' personal information. Enhancements to Staples' existing privacy policy would bring more transparency to its personal information management practices and by extension, provide customers with a level of assurance that their privacy expectations are being met (see paragraphs 35 to 38).

Process for managing privacy breaches is in place

19. A privacy breach is the unauthorized access to, use or disclosure of, personal information. A breach can occur when personal information is stolen, lost or inadvertently shared. It may also be a consequence of a deficient business procedure or operational weakness.

20. Although PIPEDA does not place any requirements on an organization with respect to privacy breaches, a key element of managing privacy is the ability to identify and respond to such occurrences. This Office has issued guidance to organizations in this regard. The guidance document outlines four steps to consider when responding to a breach or suspected breach: (1) containment and preliminary assessment; (2) evaluation of the risks associated with the breach; (3) notification of those affected; and (4) prevention of recurrence.

21. Staples has established a process to address breaches involving corporate or client information. This process is outlined in its internal privacy policy and guidance material. Should employees become aware of any circumstances to suggest Staples' systems or information has—or may have—been compromised, they are instructed to report it immediately to the Information Systems (IS) Support Centre. If the Centre cannot be reached, the employee is directed to contact Staples' CPO. All of the managers and staff we interviewed were aware of the breach management process.

22. All efforts to contain and mitigate breaches are coordinated by Staples' Head Office. Responsibility for managing breaches and providing instruction to staff rests with either the CPO, National Director of Operations or the IS Support Centre, depending on the nature of the incident. Each breach is assessed on a case-by-case basis, including whether notification of affected individuals is required. Although there was no formal privacy breach policy in place, the CPO informed us that all incidents are analyzed for the purpose of identifying and addressing the root cause. Root cause resolution may not be necessary if the incident was unlikely to reoccur or there is insufficient information to assess the root cause despite reasonable efforts. There may also be occasions where the root cause is resolved at the breach containment stage. If an investigation reveals that a breach was the result of a policy or procedural weakness, corrective measures are communicated in a notice to all stores.

Compliance monitoring activities need to be strengthened

23. Organizations are accountable for compliance with the principles listed in Schedule 1 of the *Act*. To provide assurance that its compliance obligations are met, there must be a vehicle to measure performance. We examined whether Staples performs regular self-assessments of its personal information handling practices. We reviewed internal audit records and interviewed store managers.

24. We were informed that each retail outlet is audited at least once during the calendar year. The audit template used to assess store performance focuses on theft prevention, processing of transactions, receipt and transfer of inventory, and general operations. The audits also measure compliance with established security procedures and controls designed to protect customer data, such as:

    - ensuring personal information and customer computers are stored in secure areas;
    - returned products with data storage capabilities have been processed by the Technology (Service) Centre prior to resale; and
    - customer data is not backed up on any store machine or drive.

25. In terms of data storage devices, Staples' returns policy stipulates that a manager must verify that a device has been wiped prior to resale. We found that this is not consistently done. In clearing an item for resale, most managers assume the wipe-and-restore process has been effective. Fourteen of the 17 stores we examined confirmed that random inspections are not carried out, and devices destined for resale are not tested as part of the internal audit process.

26. Privacy protection also includes limiting the collection of personal information to what is legitimately necessary, ensuring the information is not used or disclosed for purposes other than those for which it was collected (except with consent or as required by law), and destroying the information when it is no longer required. We found that Staples was unable to provide records to demonstrate that its collection, retention and disposal of personal information is subject to formal internal reviews. Moreover, although a privacy breach process is in place, there is no compliance monitoring to ensure that corrective measures taken fully address the breach.

27. An ongoing monitoring strategy, including internal audits, would provide a means of mitigating privacy risks and provide a level of assurance that the principles listed in Schedule 1 of the *Act* are integrated in Staples' day-to-day operations.

28. RECOMMENDATION

- Staples should include privacy specific compliance reviews as part of its internal audit program.

Staples' response:

The company agrees with the recommendation.

The company has made changes to its loss prevention audit checklist to address the storage, collection, retention and disposal of personal information and other privacy related items in more depth.

The company has established a program of weekly tech room inspections to further ensure privacy compliance. In addition, the company is conducting tech room privacy training in all of its stores to reinforce best privacy practices with respect to customer returns and repairs. The company has implemented Code of Ethics and Personal Information Management training, mandatory for all associates, which reinforces privacy protection priorities.

The company has centralized data recovery services to avoid having its stores retain customer data in its technical services area. The company further developed and released an automatic application that identifies files (that may belong to customers) inadvertently stored on tech room computers. All files so identified are removed in support of the company's policy not to retain customer data in its stores.

The company will continue to identify additional compliance reviews to support its privacy policies. The company has established a cross-functional privacy governance team to oversee privacy compliance.

LIFE CYCLE MANAGEMENT OF PERSONAL INFORMATION

29. The *Act* establishes the rules for managing personal information under an organization's control. It balances the need for businesses to collect, use and share personal information for legitimate purposes with an individual's right to privacy. In summary, organizations covered under PIPEDA are required to:

    - clearly identify the purpose(s) of the collection before or at the time of collection;
    - obtain consent for the collection, use and disclosure of personal information;
    - limit the information being collected to the minimum required to meet the identified purposes;
    - use and disclose the personal information only for the purpose for which it was collected; and
    - retain personal information only for as long as necessary.

30. We looked at how Staples manages personal information to assess the extent to which it is meeting the above obligations. In addition to its policies and procedures, we examined the processes for handling personal information within Staples' various business areas, from the time of collection until disposal.

Customers are not always informed of the purpose of collection

31. Staples collects personal information about its customers at the point of sale, as well as part of the copy, return and repair processes. The data collected is generally limited to name, address, telephone number and payment information (i.e., credit card or debit card number). When a device with data capture capability is returned for repair or refund, the customer's password is also collected to facilitate access to the device. In addition, personal information is collected from those seeking to obtain one of Staples' credit card products, including the applicant's name, address, date of birth, social insurance number (optional), employment and financial information.

32. PIPEDA requires the knowledge and consent of individuals for the collection, use and disclosure of their personal information. In order for consent to be meaningful, the *Act* requires that the purpose(s) for the collection, use and disclosure be clearly stated.

33. Staples' privacy policy states that it will only collect and use personal information about its customers to identify and communicate with them, to protect the Organization and customers against error and fraud, and to provide information to customers about products and services. The policy also states that customers' personal information will not be used for any other purpose, nor will it be disclosed to third parties without consent.

34. Although the purposes of collection are addressed in policy, they are not included on some of the forms used to collect customer data. While it is reasonable to presume that customers would understand the rationale for collecting contact information (i.e., name, address and telephone number) for delivery of product orders and to facilitate the return of an item under repair, they may not be aware that information collected for the purpose of issuing a refund may also be used for fraud detection. To ensure customers are fully informed, all documents used to collect personal information should clearly state the purpose of the collection and the uses that will be made of the information.

There is a lack of transparency surrounding trans-border data flows

35. Trans-border flows of personal information are common in today's global economy. As many organizations operate internationally, personal information may be collected in one jurisdiction and transferred to another for processing and storage. These data transfers occur for various reasons, including the availability of service providers, to enhance customer service or to increase operational efficiency. PIPEDA does not prohibit trans-border data flows for legitimate business purposes; it does however require organizations to be open about such practices.

36. We reviewed Staples' business processes and forms, its privacy policy and notices posted on its website regarding online purchases. Our inquiries revealed that supply orders received by Staples' call centres, as well as records captured through its online copy/print service, are transmitted and stored in the United States. These records may contain personal information. We found no evidence that customers are informed of these data transfers, nor did Staples provide information that they were.

37. The privacy principles embodied in Schedule 1 of the *Act* are designed to provide individuals control over how their personal information is handled. Individuals have a right to be informed that personal data may be processed or stored in another country and may be accessible to authorities within that jurisdiction. While some may be willing to accept a degree of risk in return for access to a particular product or service, they should be equipped with sufficient information to make an informed decision.

38. Where applicable, Staples has an obligation to inform its customers that personal information may be accessible to law enforcement and national security authorities in foreign jurisdictions. Such notification should be clear and understandable, and given at the time personal information is collected.

Collection extends beyond what is required to assess credit risk

39. The life cycle management of personal information begins with its collection. Organizations subject to PIPEDA must ensure that they limit the collection of customers' data to what is necessary for legitimate business purposes.

40. As reported in paragraph 31, Staples collects personal information about customers through its sales, returns, repairs, copy service and credit application processes. We expected these collection activities to be both relevant and not excessive.

41. We found Staples' collection practices are in keeping with the limiting collection principle, with one exception. We noted that some stores collect photocopies of government-issued identification as part of the instant (in-store)

credit program, notwithstanding company policy that prohibits this collection. These records—which included driver's licences, health cards and passports—were attached to credit application forms.

42. Government-issued identification documents contain a significant amount of personal information. In addition to name, they may include the individual's address, nationality, date of birth, a photograph and some physical descriptions (e.g., height and eye colour).

43. Credit card issuers have a legitimate need to collect personal information in order to identify and evaluate an applicant. While the collection of an individual's financial liabilities, source and amount of income is required to assess credit risk, a description of the applicant's physical characteristics is not.

44. Moreover, there is a difference between examining a document, recording information from it, and retaining a copy of the entire record. Even if there is a requirement to record certain information for identification purposes, photocopying the document is an excessive collection of personal information.

45. We observed another practice regarding instant credit applications that warrants attention. Once the application has been completed, the information contained therein is supplied to the credit card issuer for assessment purposes. Almost three-quarters of the stores we visited were conveying this information by telephone while on the sales floor. Such a practice could potentially expose the applicants' personal information to bystanders. Staples' sales and service associates should be guided accordingly.

46. Separate but related to this, we found that in-store credit applications, both approved and denied, were retained by many stores indefinitely. This practice ceased during the course of the audit.

Opt-in (express) consent is obtained for marketing purposes

47. Organizations subject to PIPEDA can only use and disclose personal information for the purpose for which it is collected, except with the consent of the individual or where required by law. An organization may seek consent by using either a positive/opt-in or a negative/opt-out mechanism.

48. Under the opt-in form of consent, commonly referred to as "express consent," the individual must give the organization permission to use or disclose personal information for secondary purposes. Secondary purposes are additional to those for which the information was originally collected. Unless the consumer takes action to opt-in (says "yes") the organization does not assume consent. Conversely, under the opt-out mechanism, the individual must express their non-agreement to the secondary purpose; unless the individual takes action (says "no" to it) the organization assumes consent and proceeds with the proposed use or disclosure of personal information.

49. We examined Staples' business processes and the forms used to collect personal information. We found that consumers' personal data is collected solely for the purpose of service delivery. Staples has adopted, as company policy, opt-in (express) consent for the secondary use of personal information for marketing purposes. Business forms, in both hard copy and electronic formats, contain a box that consumers must check if they wish to receive marketing products (e.g., notice of special offers and new products, electronic flyers, catalogues, etc.). If the individual omits to check the box, Staples assumes the consumer has not consented to the secondary use. The organization has also established an ongoing mechanism for withdrawing consent at any time.

Records attached to print/copy orders are retained longer than necessary

50. The *Act* stipulates that an organization shall only retain personal information for as long as necessary to fulfill its purpose. We expected Staples to have mechanisms in place to meet this obligation. We reviewed its retention policy and schedule, as well as associated procedures.

51. We found documents that were not covered by the retention and disposal schedule, records that were kept beyond their scheduled disposal dates, and others that were assigned excessive retention periods (i.e., kept indefinitely). During the course of the audit, Staples revised its retention and disposal schedule; records previously omitted were added to the schedule and the retention period for certain records was shortened. Notwithstanding these efforts, the retention period for one category of records remains excessive.

52. Staples' Copy and Print Centre offers an online service. A request order—with the material to be printed attached—is submitted electronically using a web-based document submission service that connects a customer's computer directly to the Print Centre's network. An automated email is generated when the order is ready for pick up. Records attached to online print/copy orders are retained in Staples' database for one year.

53. We were informed that the records are kept to facilitate the processing of subsequent orders for the same material. While the practice may have merit in terms of meeting the needs of business clients (some of whom routinely re-order business forms, envelopes and letterhead), the retention of personal information—e.g., resumés, legal documents such as divorce and custody agreements—on the basis that it may have some future use is not in keeping with the limiting retention principle.

54. Under PIPEDA, Staples is obligated to dispose of personal information when it is no longer required for the purpose for which it was collected. Once a print/copy request order has been processed and the customer is satisfied with its quality, the purpose of the collection has been fulfilled. Any further retention should be with the customer's express consent.

There is no follow-up to verify that data has been wiped on leased business machines

55. Staples' retail outlets lease photocopiers to deliver their copy and print services. Some of these machines have built-in hard drives that retain images of the copied documents. When these copiers reach the end of lease or they are replaced because they cannot be repaired, they are returned to the supplier. We looked at whether existing controls provide assurance that the hard drives on these machines are wiped or destroyed.

56. We examined records related to the leasing arrangements and interviewed employees within Staples' Copy and Print Centres. According to lease records and verified through our discussions with staff, the supplier is responsible for the integrity of data residing on the equipment. This includes ensuring the hard drives are wiped prior to disposal, recycling or reuse. Staples confirmed that it relies upon the assurances provided by the supplier in this regard; it does not conduct any independent follow-up to ensure its customers' data has been erased.

57. Monitoring compliance with the leasing arrangements presupposes a mechanism that tracks the wiping or destruction process. Under existing arrangements suppliers are not required to submit a signed declaration to Staples, recording the date upon which a hard drive is wiped or destroyed. Requiring the production of the declaration, commonly referred to as a record of destruction, would demonstrate that Staples is exercising due diligence in protecting its customers' personal information.

58. RECOMMENDATIONS

In keeping with the code of fair information practices listed in Schedule 1 of PIPEDA, Staples should:

- make clients aware of all potential uses and disclosures of their personal information, including any data transfers to foreign jurisdictions;

Staples' response:

The company agrees with the recommendation.

The company will make appropriate changes to its corporate privacy policy by May 15, 2011.

- not collect and retain copies of government-issued identification as part of its in-store credit program;

Staples' response:

The company agrees with the recommendation.

The company's current policy prohibits copying and retaining government–issued identification for any reason. The company has re-communicated this to its stores and hereafter will continue to enforce this policy.

- ensure the processing of in-store credit applications is conducted in a private area;

Staples' response:

The company agrees with the recommendation.

The company has issued a directive to its stores reminding store associates of the obligation to maintain the privacy of all aspects of the credit application process and will continue to enforce this policy.

- limit the retention of personal information that accompanies online print/copy orders to a period that allows the client to review and address any issues related to print quality;

Staples' response:

The company agrees that customers should be aware that online submissions will be stored for one year.

The company feels that the retention of customers' online submissions for a period of one year is appropriate for consumers, as well as businesses, since the information is stored securely by a third party under appropriate agreements and restrictions. The only person who can trigger the re-use or disclosure of the information is the customer. However, the company will provide suitable notice to customers regarding such retention, thereby enabling the customer to opt to use over the counter copy services as an alternative.

- ensure that lease agreements with equipment suppliers include a requirement that the supplier issue Staples a certificate of destruction, confirming the date the hard drive was wiped or destroyed.

Staples' response:

The company agrees with the recommendation.

The company will require certificates of destruction from its copy equipment suppliers. This requirement has been communicated to existing suppliers and will be embedded in all new agreements with suppliers as they are initiated or renewed.

SAFEGUARDING CUSTOMERS' PERSONAL DATA

59. Organizations subject to PIPEDA are required to protect personal information by implementing safeguards that are proportionate with the sensitivity of the information held. Appropriate measures and controls must be present to ensure personal information is not subject to unauthorized access, use, disclosure, alteration or destruction.

60. We expected Staples to have sufficient physical, technical and organizational mechanisms to maintain the integrity and confidentiality of its customers' personal information. We examined its policies, procedures, processes, third party agreements and IT system access controls. We also conducted physical inspections at selected stores.

Personal information found on data storage devices destined for resale

61. As previously mentioned, this Office investigated Staples on two occasions where it was alleged that Staples failed to protect personal information under its control. In both instances a device with data capture capabilities was returned with personal information about the purchaser residing on it. Staples resold the devices without erasing the data. This Office found that Staples had failed to adequately safeguard the complainants' personal information and that these privacy breaches were the result of ineffective procedures and controls surrounding the management of returned data storage devices. In responding to the last complaint Staples agreed to implement a full "wipe-and-restore" procedure on all returned data storage devices. We, therefore, expected to find that Staples had implemented an effective process to mitigate the risk of another data breach.

62. In November 2009, Staples revised its procedures for managing returned data storage devices. According to these procedures, a returned device is tagged and stored in a cabinet pending a diagnostic assessment. The assessment determines whether the device is resalable or is to be returned to the vendor (RTV). Whether destined for resale or RTV, the device is processed in the same manner. A wipe-and-restore procedure is performed and the technician must certify, in writing, that the procedure has been completed. The device is then forwarded to a manager for sign-off. The manager's sign-off serves as verification that the device has been processed in accordance with established procedures. A label is affixed to the device—reflecting that it has been processed—and it is either restocked or placed in an RTV bin.

63. While the revised procedures include key control mechanisms, they are not consistently applied. In 15 of the 17 stores audited we noted instances where data storage devices were:

- resealed and verified as being wiped when such was not the case;
- not verified by a manager prior to being restocked; or,
- sent directly to the RTV bin without being processed (wiped) by a technician.

64. We carried out audit tests at each of the stores visited. A sample of 149 data storage devices that had undergone Staples' wipe-and-restore process and were packaged for resale was selected for this purpose. The sample included desktop computers, laptops, USB hard drives, internal hard drives, memory sticks and memory cards.

65. Each device was plugged into a laptop and viewed using Windows™ Explorer. Some of the devices had accessible files containing personal information that was readily visible, while the remaining devices appeared to be wiped i.e., contained no customer data (this is data introduced onto the device, intentionally or otherwise, by or for the customer). Those appearing to be wiped were then examined for hidden content using readily available software (freeware) that was downloaded from the Internet at no cost.

The wiping process overwrites the content of the space previously occupied by the data. Unless a device is wiped, data previously "deleted" may be recovered using readily available tools that can restore it into a readable format.

66. When customer data is "deleted" on a data storage device, it is not actually removed. The location where the data resided is simply re-allocated as free space. In other words, the information the hard drive requires to find the data is deleted, not the data itself. To ensure that customer data is securely erased, it must be wiped. Security tools and software are available—and additional programmes may be developed—for this purpose. We tested each device within the audit sample to determine whether customer data was fully wiped. The results are provided below.

67. In summary, we found that 54 of the 149 devices tested contained customer data. A number of these devices contained personal information that included government-issued identification numbers, email messages, personal correspondence and photographs, immigration documents, resumés, financial statements, custodial arrangements and personal contact lists.

68. We also examined a sample of digital cameras, global positioning systems (GPS) and portable media players/personal digital assistants. The cameras and media players were cleansed of all residual data. Two of eight GPS units were not reset to factory settings, thereby exposing the trip histories and home addresses of the previous owners.

69. The audit shows that Staples did not ensure data storage devices are wiped of all customer data prior to resale. There are two contributing factors. As noted in paragraph 63 established procedures for processing returned devices are not consistently followed. Moreover, the procedure used to process a device varies upon the manufacturer and in some instances is not effective in wiping all customer data. In summary, our testing demonstrates that the revised procedures have not been effective in addressing the deficiencies that existed in 2008. Until this is addressed, the privacy of Staples' customers will remain at risk.

Device	Number Tested	No Customer Data Found	Customer Data Found
Desktops and Laptops	20	3	17
USB Hard Drive	55	36	19
Internal Hard Drive	10	9	1
Memory Stick	20	12	8
Memory Card	44	35	9
Total	149	95	54

70. RECOMMENDATION

- Staples should review its procedures and processes for wiping data storage devices and implement enhanced controls to eliminate any risk of personal information being disclosed.

Staples' response:

The company agrees with the recommendation.

In response to a 2008 complaint, the company implemented a policy of wiping and restoring all returned product (with memory) prior to reselling such product. In the case of desktop and laptop computers, the company's wipe-and-restore process follows procedures and uses tools provided by manufacturers. Such procedures preserve only the original factory shipped software. Despite the manufacturers' warnings that this process will erase all files, data is in fact recoverable by using forensic software. No manufacturer recommends the over-writing of data as part of its recommended wipe-and-restore process. Overwriting processes may also damage a computer's hard drive and destroy the original factory-shipped software (including manufacturers' wipe-and-restore tools), rendering the universal use of such a process commercially unviable.

During the course of the audit by The Office of the Privacy Commissioner, the audit team was able to recover data from some computers that had undergone the manufacturers' recommended wipe-and-restore process, using forensic software. The audit team recommends a wipe-and-restore process that "overwrites" all the customer data to the extent that no customer data is recoverable.

The company is actively testing several means of wiping data from returned product (to the point that data is not recoverable using forensic software) without damaging or destroying hard drives, valuable operating systems and other manufacturer provided tools.

Personal Information found on some devices packaged for resale:

- Names, addresses, social insurance numbers, provincial health card and passport numbers;
- Employment history, diplomas and academic transcripts;
- Personal investment holdings, banking information, credit card statements and tax records;
- Driver's licences, permanent resident cards and student visas.

Documents containing customer's personal information are not always stored securely

71. Staples retail outlets and corporate assets are controlled by various means, including security cameras and intrusion detection systems, anti-theft devices, the use of locked cabinets and other techniques to control access to restricted areas.

72. Customer data is generally retained in the technology centre, administration office and shipping and receiving dock. With the exception of the latter, entry to these areas is controlled through the use of locked doors, keys or coded access pads.

73. Staples' policy requires that all personal information be secured, in either a locked cabinet or room, when not in use. Twelve of the 17 stores we visited were in noncompliance with the policy. We found delivery, transfer and special order forms stored in unlocked filing cabinets.

74. We also found that return and repair forms were not adequately protected in approximately one-third of the stores visited. Moreover, returned data storage devices were kept in unlocked cabinets, on open shelves or were left unattended on service counters. These items are particularly vulnerable as they are not equipped with anti-theft protection. Left unattended in an unsecure environment, they could be stolen.

Customer data discarded in wastebaskets and recycling bins

75. Organizations have an obligation to ensure personal information is disposed of in a secure manner. We examined Staples' procedures for managing records that are no longer required. We found that customer data is generally disposed of on-site under contract with a records destruction company. Each store is equipped with locked shredding containers for this purpose. We found instances where order forms containing personal information were discarded in wastebaskets or recycling bins, rather than in a shredding container.

76. Poor disposal practices have been the source of privacy incidents in other entities. Organizations have an obligation to ensure that personal information is protected throughout its entire life cycle—from the time of collection until it is disposed of using a secure method. While not appearing as systemic, there is evidence that some employees are not cognizant of the importance of handling personal information with care.

Shared user identification and passwords puts customer data at risk

77. Controlled access to an IT system and the data stored within represents a key safeguard in protecting privacy. It mitigates the risk of personal information being compromised—inappropriately used, disclosed, modified or deleted—by restricting access to those with a legitimate need. We expected system access rights to be in keeping with the need-to-know principle and controlled by a user authentication process (i.e., user ID and password).

78. Staples informed us that access rights are issued according to an employee's role and responsibilities. A manager's profile differs from that of a service technician. Similarly, sales associates have access to purchase and delivery orders; they do not have access privileges to repair orders or records generated by the Copy and Print Centres.

79. While system access profiles are an essential component of IT security management, they are ineffective unless supplemented by a strong user authentication process. We found that common user accounts have been established in various departments, with employees sharing the same user identification and password. The majority of stores visited had at least one computer terminal with the authentication credentials (user identification and password) affixed to the screen or in clear view of customers. Moreover, we found terminals on the sales floor were left unattended and remained open (logged on).

80. Logging user activities is required to determine whether access rights have been appropriately exercised. With the issuance of common user names and passwords, Staples lacks this capability. Without a means of monitoring system access, Staples cannot be assured, with a reasonable degree of certainty, that customer data is used and disclosed for legitimate purposes in all instances.

81. RECOMMENDATIONS

To safeguard customer information, Staples should ensure that:

- personal information is stored in locked cabinets or secured areas, as required by its policy;

Staples' response:

The company agrees with the recommendation.

The company has re-communicated and hereafter will continue to enforce its policies with respect to personal information storage and has included this matter in its internal audit procedures.

- staff are reminded of the importance of using secure methods to destroy customer data; and

Staples' response:

The company agrees with the recommendation.

The company has re-communicated and hereafter will continue to enforce its policies with respect to customer data destruction and has included this matter in its internal audit procedures.

- employees have unique system access credentials to facilitate user accountability and mitigate the risk of unauthorized access to customer data.

Staples' response:

The company agrees with the recommendation.

The company continues to look for practical systems access security solutions and it is expected that an application under current development will enable individual secured access.

It should be noted that the company's current policy prohibits the storage of personal identifiable information on any shared network other than those systems required for operational purposes. In addition, access control policies regarding the point-of-sale server in retail store front offices are in place and are subject to audit review. The company systems also provide for automatic logouts and the rotation of generic passwords.

Conclusion

82. The *Personal Information Protection and Electronic Documents Act* (PIPEDA or the *Act*) imposes obligations on private sector organizations in respect of the management of personal information. The Act balances an individual's right to privacy with the need for organizations to collect, use and disclose personal information for legitimate purposes.

83. In the course of conducting its business, Staples handles a significant amount of personal information. While contact information—name, address, telephone number and payment data—about its customers is at the core of Staples' collection activities, it is entrusted with information that extends beyond its day-to-day business requirements. Online copy/print orders can include resumés and legal documents such as divorce settlements and custody arrangements. A returned computer or one under repair may contain details about an individual's academic background, medical conditions or personal financial information.

84. PIPEDA requires organizations to manage personal information in accordance with the 10 principles of Schedule 1 and be responsible for the personal information under their control. In this regard, Staples has implemented policies and procedures to manage its information holdings. Roles and responsibilities are clearly defined and understood throughout the organization. Various mechanisms are used to enhance privacy awareness amongst staff, including mandatory training. Staples could, however, benefit from an ongoing monitoring strategy to ensure that these practices are adhered to across the organization.

85. Staples' collection, use, retention and disposal practices are generally in keeping with PIPEDA requirements. While we noted exceptions, Staples limits the collection and use of personal information to what is required for business purposes, and ensures that it has an individual's express consent for any secondary use of the information for marketing purposes. However, we found Staples is not transparent with respect to personal information being transferred to a foreign country for processing. While PIPEDA does not prohibit trans-border data flows, it does require organizations to be open about such practices.

86. Ineffective processes and procedures surrounding data storage devices were the subject of two previous complaints filed against Staples with this Office. These complaints involved privacy breaches, where personal information on data storage devices had not been adequately erased prior to being resold, resulting in the improper disclosure of personal information to other customers. Staples committed to taking corrective action, including implementing a full "wipe-and-restore" procedure on all returned data storage devices. While Staples had enhanced its procedures and control mechanisms in response to the complaints, our audit found that they have not been effective in all cases since then. In summary, the deficiencies that existed in 2008 persist today, continuing to place personal information at risk. Until this matter and the other recommendations in this report are addressed, Staples will not meet its obligations under PIPEDA.

About the Audit

AUTHORITY

Section 18 of the *Personal Information Protection and Electronics Documents Act* (PIPEDA or the *Act*) empowers the Privacy Commissioner to undertake an audit of the personal information management practices of an organization if the Commissioner has reasonable grounds to believe that a contravention of the *Act* is occurring.

OBJECTIVE

The objective was to assess whether Staples has implemented adequate controls to protect personal information about its customers (including personal information that resides on returned data storage devices), and whether its policies, processes and practices for managing such information comply with the 10 privacy principles listed in Schedule 1 of PIPEDA.

CRITERIA

We expected Staples to have implemented policies and processes that comply with the requirements of the collection, consent, use, disclosure and retention principles established under Schedule 1 of PIPEDA (Appendix B). Specifically, PIPEDA requires that:

- the purpose of collection of personal information be identified at or before the time of collection;
- consent of the individual be obtained prior to collection, use or disclosure of personal information;
- the collection of personal information be limited to that which is necessary for the purposes identified by the organization;
- personal information be used and/or disclosed only for the purposes for which it was collected, except with the consent of the individual or as required by law; and
- personal information be retained only as long as necessary.

As per the requirements of the Safeguards Principle under PIPEDA, Staples is required to have appropriate measures in place to protect the personal information under its control.

Finally, in accordance with the Accountability and Openness Principles under PIPEDA, Staples is required to:

- define roles and assign responsibilities for privacy compliance throughout the organization;
- implement policies and procedures that give effect to the 10 principles listed in Schedule 1 of the *Act*; including staff training; and
- make readily available specific information about it policies and procedures relating to the management of personal information.

SCOPE AND APPROACH

The audit commenced with a survey of Staples' personal information management practices. This included discussions with officials at Staples Head Office and visits to two of its retail outlets. A purposive sample strategy was used to establish the audit program, with consideration given to geographical locations and store volumes. Two regional repair depots, one call center, an online discount facility and 17 stores were selected for audit examination.

Audit evidence was obtained through various means, generally involving on-site examinations, interviews and information obtained through correspondence. We also reviewed policies, procedures, agreements, process-flow documents, training materials and IT system access controls. Finally, we tested returned data storage devices destined for resale or return to the manufacturer to ascertain whether they contained personal information (were wiped and restored).

The audit did not assess or compare Staples personal information management practices with practices or standards that may be followed by other retailers.

Audit activities were carried out in the National Capital Region and in seven provinces. The audit work was substantially completed on December 31, 2010.

STANDARDS

The audit was conducted in accordance with the legislative mandate, policies and practices of the Office of the Privacy Commissioner, and followed the spirit of the audit standards recommended by the Canadian Institute of Chartered Accountants.

AUDIT TEAM

Director General: Steven Morgan

Garth Cookshaw
Dan Bourgeault
Bill Wilson

Appendix A – Recommendations and Responses

RECOMMENDATION

1. Include privacy specific compliance reviews as part of its internal audit program.

Staples' response:

The company agrees with the recommendation.

The company has made changes to its loss prevention audit checklist to address information storage, collection, retention and disposal of personal information and other privacy related items in more depth.

The company has established a program of weekly tech room inspections to further ensure privacy compliance. In addition, the company is conducting tech room privacy training in all of its stores to reinforce best privacy practices with respect to customer returns and repairs. The company has implemented Code of Ethics and Personal Information Management training, mandatory for all associates, which reinforces privacy protection priorities.

The company has centralized data recovery services to avoid having its stores retain customer data in its technical services area. The company further developed and released an automatic application that identifies files (that may belong to customers) inadvertently stored on tech room computers. All files so identified are removed in support of the company's policy not to retain customer data in its stores.

The company will continue to identify additional compliance reviews to support its privacy policies. The company has established a cross-functional privacy governance team to oversee privacy compliance.

RECOMMENDATION

2. Staples should make clients aware of all potential uses and disclosures of their personal information, including any data transfers to foreign jurisdictions.

Staples' response:

The company agrees with the recommendation.

The company will make appropriate changes to its corporate privacy policy by May 15, 2011.

RECOMMENDATION

3. Staples should not collect and retain copies of government-issued identification as part of its in-store credit program.

Staples' response:

The company agrees with the recommendation.

The company's current policy prohibits copying and retaining government–issued identification for any reason. The company has re-communicated this to its stores and hereafter will continue to enforce this policy.

RECOMMENDATION

4. Staples should ensure the processing of in-store credit applications is conducted in a private area.

Staples' response:

The company agrees with the recommendation.

The company has issued a directive to its stores reminding store associates of the obligation to maintain the privacy of all aspects of the credit application process and will continue to enforce this policy.

RECOMMENDATION

5. Staples should limit the retention of personal information that accompanies online print/copy orders to a period that allows the client to review and address any issues related to print quality.

Staples' response:

The company agrees that customers should be aware that online submissions will be stored for one year.

The company feels that the retention of customers' online submissions for a period of one year is appropriate for consumers, as well as businesses, since the information is stored securely by a third party under appropriate agreements and restrictions. The only person who can trigger the re-use or disclosure of the information is the customer. However, the company will provide suitable notice to customers regarding such retention, thereby enabling the customer to opt to use over the counter copy services as an alternative.

RECOMMENDATION

6. Staples should ensure that lease agreements with equipment suppliers include a requirement that the supplier issue Staples a certificate of destruction, confirming the date the hard drive was wiped or destroyed.

Staples' response:

The company agrees with the recommendation.

The company will require certificates of destruction from its copy equipment suppliers. This requirement has been communicated to existing suppliers and will be embedded in all new agreements with suppliers as they are initiated or renewed.

RECOMMENDATION

7. Staples should review its procedures and processes for wiping data storage devices and implement enhanced controls to eliminate any risk of personal information being disclosed.

Staples' response:

The company agrees with the recommendation.

In response to a 2008 complaint, the company implemented a policy of wiping and restoring all returned product (with memory) prior to reselling such product. In the case of desktop and laptop computers, the company's wipe-and-restore process follows procedures and uses tools provided by manufacturers. Such procedures preserve only the original factory shipped software. Despite the manufacturers' warnings that this process will erase all files, data is in fact recoverable by using forensic software. No manufacturer recommends the overwriting of data as part of its recommended wipe-and-restore process. Overwriting processes may also damage a computer's hard drive and destroy the original factory-shipped software (including manufacturers' wipe-and-restore tools), rendering the universal use of such a process commercially unviable.

During the course of the audit by the Office of the Privacy Commissioner, the audit team was able to recover data from some computers that had undergone the manufacturers' recommended wipe-and-restore process, using forensic software. The audit team recommends a wipe-and-restore process that "overwrites" all the customer data to the extent that no customer data is recoverable.

The company is actively testing several means of wiping data from returned product (to the point that data is not recoverable using forensic software) without damaging or destroying hard drives, valuable operating systems and other manufacturer provided tools.

RECOMMENDATION

8. Staples should ensure that personal information is stored in locked cabinets or secured areas, as required by its policy.

Staples' response:

The company agrees with the recommendation.

The company has re-communicated and hereafter will continue to enforce its policies with respect to personal information storage and has included this matter in its internal audit procedures.

RECOMMENDATION

9. Staples should ensure that staff are reminded of the importance of using secure methods to destroy customer data.

Staples' response:

The company agrees with the recommendation.

The company has re-communicated and hereafter will continue to enforce its policies with respect to customer data destruction and has included this matter in its internal audit procedures.

RECOMMENDATION

10. Staples should ensure that employees have unique system access credentials to facilitate user accountability and mitigate the risk of unauthorized access to customer data.

Staples' response:

The company agrees with the recommendation.

The company continues to look for practical systems access security solutions and it is expected that an application under current development will enable individual secured access.

It should be noted that the company's current policy prohibits the storage of personal identifiable information on any shared network other than those systems required for operational purposes. In addition, access control policies regarding the point-of-sale server in retail store front offices are in place and are subject to audit review. The company systems also provide for automatic logouts and the rotation of generic passwords.

Appendix B – Principles under Schedule 1 of PIPEDA considered during this audit

4.1 PRINCIPLE 1 — ACCOUNTABILITY

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

4.1.1

Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2

The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

4.1.3

An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.

4.1.4

Organizations shall implement policies and practices to give effect to the principles, including

(a) implementing procedures to protect personal information;

(b) establishing procedures to receive and respond to complaints and inquiries;

(c) training staff and communicating to staff information about the organization's policies and practices; and

(d) developing information to explain the organization's policies and procedures.

4.2 PRINCIPLE 2 — IDENTIFYING PURPOSES

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

4.2.1

The organization shall document the purposes for which personal information is collected in order to comply with the Openness principle (Clause 4.8) and the Individual Access principle (Clause 4.9).

4.2.2

Identifying the purposes for which personal information is collected at or before the time of collection allows organizations to determine the information they need to collect to fulfill these purposes. The Limiting Collection principle (Clause 4.4) requires an organization to collect only that information necessary for the purposes that have been identified.

4.2.3

The identified purposes should be specified at or before the time of collection to the individual from whom the personal information is collected. Depending upon the way in which the information is collected, this can be done orally or in writing. An application form, for example, may give notice of the purposes.

4.2.4

When personal information that has been collected is to be used for a purpose not previously identified, the new purpose shall be identified prior to use. Unless the new purpose is required by law, the consent of the individual is required before information can be used for that purpose. For an elaboration on consent, please refer to the Consent principle (Clause 4.3).

4.2.5

Persons collecting personal information should be able to explain to individuals the purposes for which the information is being collected.

4.2.6

This principle is linked closely to the Limiting Collection principle (Clause 4.4) and the Limiting Use, Disclosure, and Retention principle (Clause 4.5).

4.3 PRINCIPLE 3 — CONSENT

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires "knowledge and consent." Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the explicitly specified and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(b) a check-off box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(c) consent may be given orally when information is collected over the telephone; or

(d) consent may be given at the time that individuals use a product or service.

4.3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

4.4 PRINCIPLE 4 — LIMITING COLLECTION

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

4.4.1

Organizations shall not collect personal information indiscriminately. Both the amount and the type of information collected shall be limited to that which is necessary to fulfill the purposes identified. Organizations shall specify the type of information collected as part of their information-handling policies and practices, in accordance with the Openness principle (Clause 4.8).

4.4.2

The requirement that personal information be collected by fair and lawful means is intended to prevent organizations from collecting information by misleading or deceiving individuals about the purpose for which information is being collected. This requirement implies that consent with respect to collection must not be obtained through deception.

4.4.3

This principle is linked closely to the Identifying Purposes principle (Clause 4.2) and the Consent principle (Clause 4.3).

4.5 PRINCIPLE 5 — LIMITING USE, DISCLOSURE AND RETENTION

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

4.5.1

Organizations using personal information for a new purpose shall document this purpose (see Clause 4.2.1).

4.5.2

Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods.

4.5.3

Personal information that is no longer required to fulfill the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information.

4.5.4

This principle is closely linked to the Consent principle (Clause 4.3), the Identifying Purposes principle (Clause 4.2), and the Individual Access principle (Clause 4.9).

4.7 PRINCIPLE 7 — SAFEGUARDS

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

4.7.1

The security safeguards shall protect personal information against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification. Organizations shall protect personal information regardless of the format in which it is held.

4.7.2

The nature of the safeguards will vary depending on the sensitivity of the information that has been collected, the amount, distribution, and format of the information, and the method of storage. More sensitive information should be safeguarded by a higher level of protection. The concept of sensitivity is discussed in Clause 4.3.4.

4.7.3

The methods of protection should include

(a) physical measures, for example, locked filing cabinets and restricted access to offices;

(b) organizational measures, for example, security clearances and limiting access on a "need-to-know" basis; and

(c) technological measures, for example, the use of passwords and encryption.

4.7.4

Organizations shall make their employees aware of the importance of maintaining the confidentiality of personal information.

4.7.5

Care shall be used in the disposal or destruction of personal information, to prevent unauthorized parties from gaining access to the information (see Clause 4.5.3).

4.8 PRINCIPLE 8 — OPENNESS

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

4.8.1

Organizations shall be open about their policies and practices with respect to the management of personal information. Individuals shall be able to acquire information about an organization's policies and practices without unreasonable effort. This information shall be made available in a form that is generally understandable.

4.8.2

The information made available shall include

(a) the name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;

(b) the means of gaining access to personal information held by the organization;

(c) a description of the type of personal information held by the organization, including a general account of its use;

(d) a copy of any brochures or other information that explain the organization's policies, standards, or codes; and

(e) what personal information is made available to related organizations (e.g., subsidiaries).

4.8.3

An organization may make information on its policies and practices available in a variety of ways. The method chosen depends on the nature of its business and other considerations. For example, an organization may choose to make brochures available in its place of business, mail information to its customers, provide online access, or establish a toll-free telephone number.