Privacy and Access Odds & Ends: Privacy Principles Edition

1. **Accountability:** This principle states that an organization is responsible for personal information under its control. The organization should designate an individual or individuals to be accountable for the organization's compliance with the principles stated in the Code. An organization needs to implement policies and practices that will help them respect the principles.
2. **Identifying Purposes:** An organization should identify the purposes for collecting information at or before the time of collection. This will enable the organization to determine which information needs to be collected in order to meet their needs. This goes hand in hand with the Limiting Collection principle (#4). Depending on the manner in which information is collected, this principle can be fulfilled orally or in writing. For example, an application form may explain the purposes of information collection to an individual.
3. **Consent:** Where it is appropriate, an individual must have knowledge of and give consent to the collection, use or disclosure of personal information. An organization should make a reasonable effort to inform individuals of the purposes for collecting information. Consent should be meaningful; the purposes should be explained in such a way that the individual can reasonably understand the use and disclosure of their personal information. Individuals are entitled to withdraw consent at any time.
4. **Limiting Collection:** Personal information should only be collected as necessary for the purposes that the organization has identified. This includes limiting the amount and type of information. The information should be collected by fair and lawful means.
5. **Limiting Use, Disclosure and Retention:** An organization should not use personal information for new purposes, unless it has the consent of the individual, or as required by law. Personal data should only be retained as long as is necessary to fulfill the organization's stated purposes. An

organization should develop specific guidelines and procedures governing the destruction of personal information.

6. **Accuracy:** In order to meet the intended purposes, personal information should be accurate, complete and up-to-date. This principle aims to minimize the possibility that incorrect information is used to make a decision about an individual. This also applies to information disclosed to third parties.
7. **Safeguards:** An organization should implement appropriate security safeguards to protect the personal information collected. The appropriate safeguard should be determined by the sensitivity, amount, distribution, format and method of storage of the information. Employees in the organization should be aware that confidentiality of personal information should be maintained.
8. **Openness:** An organization should be open about its personal information policies and practices. Individuals should be able to access an organization's policies and practices relatively easily. The method of disseminating such information depends on the nature of the organization. This may include brochures, mail to customers, online access or toll-free information lines.
9. **Individual Access:** Individuals should be informed of the existence, use and disclosure of their personal information. Individuals should have access to their personal information and be able to question and correct the accuracy and completeness of this information.
10. **Challenging Compliance:** Individuals should be able to challenge an organization's compliance with the above principles. The person accountable for an organization's compliance will be responsible for dealing with inquiries, challenges or complaints. An organization should investigate all complaints and if it is necessary, adjust its policies and practices appropriately.