island CONSORTIUM

Information Risk Assessment

Principle 1: Purpose of collection of personal information
What personal information is currently collected and used? What are the changes to personal information collected or used? What is the purpose of collecting the information? Will you be using information for a different purpose? (Why? How?)

Principle 2: Source of personal information
What is the source of personal information?

Principle 3: Collection of personal information from the subject
How are you telling the individual what you're doing with their information? Have you obtained lawful consent to process the information, in the manner in which you are using it?

Principle 4: Manner of collection of personal information
How you are collecting personal information?

Principle 5: Storage and Security of personal information
How does it flow through your company's systems? How will your project change the information flow? How you are storing and securing personal information? How long will the information be kept for? How will personal information be disposed of?

Principles 6 and 7: Access to and correction of information
Responding to people's requests for information about themselves, or requests to correct information about themselves.

Principle 8: Accuracy etc. of personal information to be checked before use
What steps do you take to check the accuracy, relevance etc of personal information before you use it? What measures are in place to ensure the information is accurate and up to date?

Principle 9: Agency not to keep personal information for longer than necessary
How long do you keep personal information and why? Are you able to erase information if requested to?

Principle 10: Use of information
What are you going to use the personal information for?

Principle 11: Disclosure of information
Who are you going to disclose the personal information to (if anyone) and why?

Principle 12: Use of Unique Identifiers
Why do you need a unique identifier, and are you allowed to use this one?

For each principle ask:
What are the risks? What is the impact on the agency or individual? What can be done to manage the risk? Will existing controls manage the risks identified? If not, what is the residual current risk? How can you further reduce or mitigate risk? Are there still risks remaining despite new safeguards?