PREPARING AN ON-LINE PERSONAL INFORMATION COLLECTION (PIC) STATEMENT AND PRIVACY POLICY STATEMENT (PPS)

WHAT IS THE DIFFERENCE BETWEEN A PIC STATEMENT AND A PPS?

- A *PIC Statement* is a statement given in compliance with the requirements of the Personal Data (Privacy) Ordinance ("the Ordinance") to notify individuals of certain matters when collecting such information from them. That is, it is a statement of a certain limited content (described below) given in relation to specific collections of recorded information from individuals about themselves.

- A *PPS* is a general statement of an organisation's privacy policy and practices that applies to the organisation's collection, holding and use of recorded information about individuals as a whole. Under the Ordinance, organisations are required to ensure that their policies and practices in this regard can be ascertained by other persons.

PIC STATEMENT

WHEN SHOULD A PIC STATEMENT BE GIVEN?

- A PIC Statement should be given whenever you collect information on-line from individuals that is about them and identifies them (so-called 'personally identifiable information'), including information about their use of your website.

- The most obvious way in which such information is collected on-line is in an on-line registration or other form. Each form of this sort should include a PIC Statement, either as part of its text or by means of a "hotlink" on the form itself.

- In addition, information may also be collected from an individual without his or her being aware of this, e.g. through the use of "cookies". For example, once an individual registers on a web site, cookies may be used to make a record of the pages he or she visits. In such a case, the PIC Statement given in the original registration form should cover the subsequent collection activities. Alternatively or in addition, a pop-up box could be used to provide a PIC Statement whenever such collection begins. If your website bars users who do not accept cookies, this should be made clear in the relevant PIC Statement.

WHAT GOES INTO A PIC STATEMENT?

- **PURPOSE STATEMENT**: This is a statement of the purposes for which the information will be used following collection. For example:

⇒ "The information collected from you will be used for the purpose of processing your purchase orders and managing your account with us." Or,

⇒ "The information about you collected by means of this form will be used only for compiling aggregate statistics about individuals registering with us."

- *TIP*: If your website has more than one on-line form, make sure the purpose statement used for each form fits the particular collection of personal data concerned.

- **STATEMENT OF POSSIBLE TRANSFEREES**: This should state the types of organisations to whom personally identifiable information collected from the individual may be disclosed.

- If you do not disclose personally identifiable information to any other party, it would be a good idea to mention this as it is likely to be favourably regarded by visitors to your website. For example:

  ⇒ "Information we collect about you will not be disclosed by us to any other party in a form that would identify you."

- If you post personally identifiable information on your website, this is a form of disclosure. Indeed, if no restrictions are placed on access to the relevant part of your website, such information could in theory be disclosed to any user of the Internet. Accordingly, such a practice should be made clear in the relevant PIC Statement.

- **STATEMENT OF RIGHTS OF ACCESS AND CORRECTION**: This should inform the individual that he or she has the right to request access to and correction of personally identifiable information about him or her that is held by you. For example:

  ⇒ "You have the right to request access to and correction of information about you held by us."

- **NOTICE OF CONTACT PERSON TO REQUEST ACCESS OR CORRECTION:** This should inform the individual of the name and contact details of the person to contact to request access to or correction. In an on-line situation this could be in the form of an e-mail address hotlinked to a pop-up message box. For example:

  ⇒ "If you wish to access or correct your personal data held by us, please e-mail winifred_chan@bonfire.com." Clicking the hotlink would activate the pop-up message box.

- **SECURITY MEASURES**: As good practice, we recommend that you also include a notice with your on-line forms on the specific security measures that are applied to on-line transmission of the form concerned. This is particularly recommended if the form is used to collect information that individuals may have security concerns about such as credit card details.

- **LINK TO PRIVACY POLICY STATEMENT:** Also as a good practice, we recommend that you provide a hotlink between your on-line forms for collecting personally identifiable information and your general Privacy Policy Statement.

PRIVACY POLICY STATEMENT (PPS)

WHEN SHOULD A PPS BE PROVIDED?

- A PPS of the sort described below is needed only if you collect information on-line from individuals that is about them and identifies them, so-called "personally identifiable information". The most obvious way in which such information is collected on-line is in an on-line registration or other form. It may also be collected from an individual without his or her being aware of this, e.g. through the use of "cookies".

- Some websites collect only aggregate information about their visitors, e.g. statistics on the number of its". As such information does not identify any particular individual, such a website does not require a PPS of the sort described below. However, Internet users may be concerned that such a website could be collecting personally identifiable information about them without their knowledge. To allay such fears we recommend that a web site of this sort include a statement on its homepage such as the following:

  ⇒ "When you visit our web site we record your visit only as a it" and do not collect any personally identifiable information from you."

- In addition if your service provider records and provides non-personally identifying information to you about visitors to your website this too should be mentioned. For example:

  ⇒ e do not collect any personally identifiable information from the visitors to our website. Our service provider makes a record of your visit that shows only the Domain Name Server address part of your e-mail address, e.g. "coolmail.com" from an e-mail address of "anon@coolmail.com", and of the pages visited. The service provider only discloses to us aggregate information about the number and types of visitors by reference to their Domain Name Server address. This information is used by us only for preparing general statistics on the usage of our website."

HOW SHOULD THE PPS BE MADE AVAILABLE?

- We recommend you make your PPS available by means of a prominent hotlink from the homepage of your website. In addition, we recommend that you provide hotlinks to your PPS from any and each form on your website that is used to collect previously identifiable information.

- *TIP*: to make your hotlink prominent try using a button marked "Privacy Policy Statement".

- More and more Internet users are looking for the privacy policies of the websites they visit before they go beyond the homepages. If you do not provide a prominent hotlink to your privacy policy from your homepage, such users may leave your website before looking further at what you have to offer.

WHAT SHOULD THE PPS CONTAIN?

- We suggest you cover the following in your PPS:

⇒ **GENERAL STATEMENT OF POLICY:** This would express your overall commitment to protecting the privacy interests of the individuals who provide information about themselves to you. For example:

  ◊ "We pledge to meet fully, and where possible exceed, internationally recognised standards of personal data privacy protection, in complying with the requirements of the Personal Data (Privacy) Ordinance. In doing so, we will ensure compliance by our staff with the strictest standards of security and confidentiality."

⇒ **STATEMENT OF PRACTICES:** This should include information on all your key practices in relation to personal data. These may include the following:

  ◊ **TYPES OF PERSONALLY IDENTIFIABLE INFORMATION YOU COLLECT AT THE WEBSITE AND THE PURPOSES YOU USE THE INFORMATION FOR:** These depend on the actual operation of the website concerned. Common types of personally identifiable information collected at websites include identification and contact details of visitors, information on their preferences in relation to the subject matter of the website and payment related information such as credit card details. Common purposes that such information is used for include the compilation of aggregate statistics on site usage, the management of accounts and processing of purchase orders. We also recommend that as far as possible websites should permit an anonymous browsing option. If you do this, say so in your PPS.

- *TIP*: You should collect only the minimum personally identifiable information necessary to carry out the purposes for which you use the information.

◊ **COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION FROM MINORS**: If your website is orientated towards, or includes content of interest to minors, include in your PPS a statement on your practices in relation to the collection of personally identifiable information from young persons. Generally, we recommend against the collection by websites of information from minors, particularly those under the age of 13, without prior consent from a person with parental responsibility for the individual, e.g. given by a parent or guardian through direct off-line contact.

◊ **COLLECTION OF INFORMATION FROM INDIVIDUALS WITHOUT THEIR KNOWLEDGE:** If you make use of technical means such as cookies to collect information from individuals without their knowledge, you should include information on this in your PPS. Matters that should be covered include:

- the circumstances under which such means are deployed;
- what information is collected by these means, in particular whether any personally identifiable information is collected;
- what the information is used for and any disclosure of the information to other parties.

You should also say whether your website allows access by users who do not accept cookies, and if it does, as we recommend it should, what loss of functionality (if any) results from not accepting cookies.

◊ **HOSTED ON-LINE STORES OR SERVICE PROVIDERS**: If your website hosts on-line stores or service providers operated by other parties, state what information you collect from your visitors who make use of such outlets for disclosure to the merchant concerned. If the privacy protection afforded to such information once it has been transferred to the merchant is outside the scope of your PPS, this should be made clear.

◊ **ACCURACY OF PERSONALLY IDENTIFIABLE INFORMATION**: Include information on measures you adopt to ensure the accuracy of personally identifiable information. In particular, if you provide an on-line facility that allows a user to correct and update his or her personally identifiable information held by you, give details of this and how it is done.

◊ **RETENTION OF PERSONALLY IDENTIFIABLE INFORMATION:** You should include information on your policies on the retention of personally identifiable information. In particular, in general terms how long such

information is retained. In addition, if you provide an on-line facility that allows a user to delete his or her personally identifiable information held by you, give details of this and how it is done.

◊ **DISCLOSURE OF INFORMATION ABOUT INDIVIDUALS**: You should state your disclosure practices. For example, many web sites do not disclose personally identifiable information to other parties or do so only with the consent of the individual concerned, e.g. to facilitate an order made by the individual with a merchant hosted at the website, except as required by law. If this is your practice, say so. Many Internet users favour websites with such a practice. Some websites disclose non-personally identifiable aggregate statistics relating to their visitors to advertisers. Again, if you do this, include it in your PPS. If your website discloses personally identifiable information or the website itself, this should be made clear. You should also provide information on any safeguards you adopt to restrict access to such information.

◊ **DIRECT MARKETING**: Do you use information collected from your visitors to market products or services to them? If so, say so and state how you go about this. In particular, state whether this is done on an opt-in or opt-out basis? You should as a minimum give individuals the opportunity to opt-out from receiving direct marketing e-mails and comply with the opt-out requests you receive. *TIP*: Many Internet users prefer to receive direct marketing materials by e-mail only on an opt-in basis.

◊ **SECURITY**: State what you do to ensure the security and confidentiality of personal data you collect on-line. For example, if you use encryption for transmission of sensitive data, which you should do, include information on this in your PPS. Other security measures to mention might include restricting access to personal data to employees who have a need to use the data and who have been trained to handle such data properly and observe confidentiality. In addition, we recommend that you also include a notice with your on-line forms on the specific security measures that are applied to on-line transmission of the form concerned. This is particularly recommended if the form is used to collect information that individuals may have security concerns about such as credit card details.

◊ **SUBJECT ACCESS AND CORRECTION**: Put in a statement on your practices in handling requests by individuals to access or correct their personal data held by you. In particular, say how you prefer to receive such requests, e.g. by e-mail, and what you require in order to satisfy yourself that the requestor is entitled to make the request. Do you handle such requests promptly and try to comply well before the expiry of the 40 day maximum period set by the Personal Data (Privacy) Ordinance. If so, say so. If you charge for complying with access requests, state your charges. *TIP*: Any such

charge must not be excessive and no charge may be levied for complying with a correction request.

◊ **CONTACT PERSON FOR ANSWERING ENQUIRIES ABOUT YOUR PRIVACY POLICY AND PRACTICES**: Include contact details of someone who will answer such enquiries. We recommend that this be in the form of an e-mail address hotlinked to a pop-up message box. For example:

⇒ "If you have any queries about our Privacy Policy and Practices, please e-mail them to winifred_chan@bonfire.com." Clicking the hotlink would activate the pop-up message box.

The above guidance is given to promote good practice in relation to on-line protection of privacy in relation to personal data and is given without prejudice to the carrying out by the Privacy Commissioner for Personal Data of any of his functions or exercising of any of his powers.

Office of the Privacy Commissioner for Personal Date - December 1998