GDPR Website Policy for [*name of service body running the website*]

1. All documents to be considered for uploading will be checked for personal data. If personal data is contained, then the website officer will consider:

   a) Why the data is in the document;
   b) Has the person whose data is disclosed given their consent for website publication. How and when was this consent obtained and how can it be revoked;
   c) Has the person seen a copy of the privacy notice surrounding the handling of their data;
   d) Has the document to be uploaded been recorded in the Website Document Publication Register;
   e) Does the document contain only the minimal amount of data required;
   f) Is the data accurate;
   g) When will this data be deleted from the website;
   h) Are the appropriate technical and organisational security measures in place;
   i) What is the perceived privacy risk to the person concerned.

   The website officer will assess whether the processing of the personal data in the document will be in accordance with the six data protection principles in the GDPR, taking into consideration the answers to these questions.

   If the website officer is satisfied that the processing will be GDPR compliant then the document may be published.

2. All documents uploaded that contain personal data will be added to the Website Document Publication Register. Recorded is the date data was received, a description of it, who/where it is from, has consent for upload been given, when is the data to be deleted by and when was it deleted securely.
   The Register is reviewed on a monthly basis to endure that is current, accurate and that deletion dates are adhered to.

3. If personal data is collected from data subjects via the website then information will be made clearly available to data subjects, telling them why their data is being collected and asking for their consent. Consent will be recorded using a positive opt in / tick box (i.e. it must not be 'pre-ticked'). Personal data will only be used for the specified purpose and not kept for any longer than needed for this purpose. If data subjects sign up to a newsletter then every newsletter / email they receive must include an 'opt out' link which makes it as easy to opt out as it was initially to sign up.

4. If, for any reason, the Web Officer is unable to access the website backend or Dropbox then the Officer with backup access to both these document storage areas will be notified and the necessary reviews and/or document deletions carried out by him/her.

5. Personal data from a public source may be uploaded only if the organisation from which it was obtained is either compliant with GDPR or the US Privacy Shield, and should only be uploaded for a purpose consistent with the purpose for its original publication.

6. Backups of the website database (i.e. all content) will be carried out monthly and the backup file stored in cloud storage [***name provider***].

7. Requests by individuals to access the personal data processed via the website should be directed to the [***named service position***]. The website officer will support them to respond to subject access requests in accordance with the data protection policy, and the GDPR.

8. Privacy notices will be supplied to all data subjects whose data is processed via the website, and also more generally via [***the service body***]. These will be published on the website. The website officer will ensure that the most recent versions are uploaded.

9. Any questions concerning this policy, or data protection in general, should be directed to the [***named service position***] ([***insert email address***])