University Web Services

Web Publishing Policy

Applicable Legislation and Policies

1. Follow both the laws and policies governing copyright infringement, intellectual property rights and other applicable laws regarding libel, privacy laws, trademarks, obscenity, computer fraud and First Amendment rights.

As a public institution, The University of Texas at Dallas provides both web access and web space to all of its students, faculty and staff. Because UTD is a publicly funded university, UTD adheres to all legal and public policy guidelines governing the administration and use of such web space.

Because state and federal legislation and the State of Texas policy outline the specific areas of liability, The University of Texas at Dallas requires that all network users follow both the laws and policies governing copyright infringement, intellectual property rights and other applicable laws regarding libel, privacy laws, trademarks, obscenity, computer fraud and First Amendment rights.

For more information, please feel free to contact Dr. Jim Gary, Information Resources Manager, at gary@utdallas.edu .

Also, if you have specific questions about security or privacy issues, please contact the Information Security Office at infosecurity@utdallas.edu.

For specific information on any of these topics, please see :

UTD Information Resources Policies
http://www.utdallas.edu/ir/policies/index.html

U. T. System Computer and Information Technology Use Policy and Guidelines
http://www.utsystem.edu/ogc/intellectualproperty/citup.htm

U. T. System Crash Course in Copyright
http://www.utsystem.edu/ogc/intellectualproperty/cprtindx.htm

Digital Millennium Copyright Act - resources from Educause
http://www.educause.edu/issues/dmca.html

2. Comply with the UTD Website Privacy Policy

Recent additions to state and federal law require changes in UTD websites in the interests of privacy, confidentiality, and security. Effective January 1, 2002, all UTD websites except *strictly* personal pages must:

A. Post a privacy statement on the departmental, school, program, research lab, etc., website that indicates what, if any, information is collected about a site visitor - including information collected by means that are not obvious (cookies, web bugs, server logs). The statement must indicate how the information is used. Include information about Section 559.003(a) of the Texas Government Code (TGC) and the Texas records retention laws (Sec. 441.180et seq. of TGC). The U. T. System site privacy policy and an example 559 and 441 TGC notice may be used as a guide. See Texas House Bill 1922 for the amended bill text.

B. Post a supplemental privacy statement specific to each web form in addition to your site policy. If you collect SSN numbers, you must indicate:

- Whether the disclosure of SSN is mandatory or voluntary.
- By what statutory or other authority the social security number is solicited.
- What uses will be made of the SSN? See text of section 7 of the Federal Privacy Act of 1974 and examples of voluntary and mandatory SSN disclosure notices .

C. Information collected must be treated as confidential and/or sensitive as defined by state and federal law and UTD policy. Texas Senate Bill 694 adds the following information to the list of confidential information as defined by Chapter 552 of the Texas Government Code (Public Information Act): a credit card, debit card, charge card or access device number, and email address.

Note: "access device" means a card, plate, code, account number, personal identification number, electronic serial number, mobile identification number, other telecommunications service, equipment, or instrument identifier or means of account access that alone or in conjunction with another access device may be used to:
a. Obtain money, goods, services or another thing of value.
b. Initiate a transfer of funds other than a transfer originated solely by paper instrument.

D. Utilize SSL encryption for all web forms. Ensure that the data collected by the form is also protected from unauthorized access from the time it is received by the webserver till it reaches the end user(s).

Sending form data to the end user(s) via plain-text email is NOT permitted - this includes as email attachments. Encrypted email may be used to transmit the data. Other methods of handling the data should be discussed with and approved by the UTD security administrator, Lea Teutsch.

To implement SSL for your forms:

If your site is hosted on the UTD UNIX web server "tangled," you simply change the links to the form page as shown below:

From: <http://www.utdallas.edu/foo/bar.html>
To: <https://www.utdallas.edu/foo/bar.html>
The change is an added "s" on the end of http.
You must block access to the form page from a non-SSL link (an <http://> link).

To do this on tangled:

a. Access your web directory on the UNIX server.
b. In the directory containing your html files with forms, create a plain text file called .htaccess.
c. Put the following statement on one line of the file: SSLRequireSSL.
d. Save the file.
e. Issue the following command: chmod 775 .htaccess.
f. You are done.

This procedure will require SSL on all pages in the directory and should only be used if you keep only html form pages in the directory.

If you require SSL on certain pages within a directory rather than all files in the directory:

a. Access your web directory on the UNIX server.
b. In the directory containing your html files with forms, create a plain text file called .htaccess.
c. Put the following in the file, one per form page:

```
<Files formpagename1.html>
SSLRequireSSL
</Files>
<Files formpagename2.html>
SSLRequireSSL
</Files>
```

d. Continue until all pages are done.
e. Save the file.
f. Issue the following command: chmod 775 .htaccess.
g. You are done.

For relative links (<A HREF="subdirectory/file.html">file</A> or <A HREF="file.html">file</A> where file refers to a page in your site's root directory), add the following to the <head> </head> section of your form pages:
<BASE HREF="http://www.utdallas.edu/yourdirecory/index.html">
where your/directory/ is the location of your site index.html page. This will prevent relative links from your SSL encrypted form page from also being SSL encrypted.

For those of you with the URL of a form page on publications, to continue to provide access to the SSL encrypted version of the form you should:
1. Change the filename of the form page and update links within you site as appropriate.
2. Create a "dummy" page with the old form page filename that contains a re-direct to the new, secure form page.
This will allow people to use the published URL, but direct them to the secure form.

If you are not hosting your site on tangled, contact your webmaster for instructions on implementing SSL.

3. Comply with the UTD Visual Identity Guidelines

The visual identity guidelines will assist webdevelopers to present a clear and consistent image in their online publications. While written with print publishing in mind, the vast majority of the guidelines apply to the web and must be followed.

4. If the site is designed for children, comply with federal and state laws designed to protect minors.