

# University System of New Hampshire e-Commerce Information Usage Statement

The security and privacy of your e-commerce transactions at the University System of New Hampshire, its colleges, and universities (collectively referred to here as USNH) are of the utmost importance to us. The following statement describes our efforts to ensure that objective.

1. Introduction
2. Information Security
3. Information We Collect
4. Our Use and Disclosure of Information
5. Links to Other Web Sites
6. Contacting Us

## **1. Introduction**

USNH provides the ability to make payments for specific charges via the Web as a convenience to community members. To ensure transactions are appropriately assigned, and to reduce the risk of fraud, USNH must collect sufficient information to positively identify users. USNH respects the privacy of your personally identifiable information. We will not sell or rent this information. However, as described in more detail in Section 3 below, there are limited circumstances in which some of your information will be by necessity, under strict restrictions, shared with third parties.

By using USNH e-commerce sites, you signify that you understand how the privacy and security of your personal information is protected and how your personal information will be used. We reserve the right, at our sole discretion, to change, modify, add, or remove portions of this statement at any time. Your continued use of the USNH e-commerce sites following the posting of any changes signifies that you are comfortable with and have accepted those changes. If you have any questions or concerns, please contact us as described in Section 6 below.

## **2. Information Security**

USNH is committed to handling your information with high standards of information security and in compliance with the USNH Information Technology Security Policy. While no computing environment is absolutely secure, we take appropriate precautions to protect the user's information. When a user submits sensitive information via the Web, that information is protected both online and off-line. We restrict access to your personally identifiable information to only employees who need to know that information in order to provide products or services to you.

### **Tips for Safe Transactions**

1. Use recent releases of browsers such as MS Internet Explorer that support an SSL encryption. Insure your operating system and browser software have the latest security updates.

2. Don't walk away from your computer when in communication with our servers.
3. Safeguard your username/password and other account information. Do not share them with others.
4. Keep personal information such as your mother's maiden name and identifying numbers (including your Social Security, driver's license, passport, and credit card numbers) in a safe and secure place. Do NOT share this information unless you know the purpose for which it will be used.
5. Before anyone else uses your computer, clear your cache or restart your browser (this eliminates copies of Web pages that have been stored in your hard drive). The preference menu in your browser can tell you how to clear your cache.
6. Always use the Exit function when ending an e-commerce session; best practice is to close the browser when the transaction is complete.
7. Practice good computer defense by installing anti-virus, anti-spyware, and firewalls.

### **3. Information We Collect**

#### **Network Information**

Occasionally network data are collected and analyzed to better help us understand how you use our web services and how we can improve our site to better meet your needs. Examples of data that may be collected include:

- IP Address
- Type of browser and operating system used to access our site
- Date and time the user accessed our site
- Information regarding which pages users access or visit

For site security purposes and to ensure that this service remains available to all users, this site may monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. If security monitoring reveals evidence of possible abuse or criminal activity, system personnel may provide the results of such monitoring to appropriate officials. Unauthorized attempts to upload or change information on this service are strictly prohibited and may be punishable under the state and federal laws and regulations including the Computer Fraud and Abuse Act of 1986 and the National, and the Information Infrastructure Protection Act of 1996.

#### **Email Information**

If you send us an electronic mail message with a question or comment that contains personally identifying information, we will only use the personally identifiable information to respond to your request and analyze trends. We may redirect your message to another government agency or person who is in a better position to answer your question. USNH strongly recommends that users not send to us via e-mail personally identifiable, financially sensitive information such as SSN, bank account or credit card information. Please contact us (See Section 6) if you receive an instruction or e-mail from someone representing him/herself to be a part of USNH making such a request.

### **Required Information**

Some users may be required to provide a valid username and password to access certain Web sites. In order to make payments you will be transferred to the USNH's e-commerce vendor's (InfiNET) Web site where you may provide checking account and/or credit card information. Credit card and bank information will not be collected or stored by USNH. This information is necessary for the e-commerce vendor to process transactions, to protect you against credit card fraud, and to contact you should the need arise in administering your account.

### **Transactional Information**

When you make a payment to a USNH entity we ask you to provide information related to each transaction such as the amount of the payment. Information provided by the user is the data needed to successfully complete a Web transaction. This information may be retained by USNH to confirm the transaction has been properly assigned.

## **4. Our Use and Disclosure of Information**

### **Internal Uses**

We use the information we collect about you in order 1) to provide our services and process your transactions and 2) to provide customer service. Specifically, we use your information to help you complete a transaction, to communicate back to you, to update you on service and benefits, and to personalize our web sites for you. We give access to personally identifiable information about our users only to those USNH employees who need to know that information in order to provide products or services to you.

### **Disclosure to Other Users**

Except as noted above for need to know employees, no other users can view your personal data.

### **Disclosure to Third Parties**

USNH will not sell, rent, or lease your personally identifiable information to others. USNH will not share any of your personally identifiable information with third parties except in the limited circumstances described below, or with your express permission (and to employees as described above), or to comply with applicable law. These third parties are limited by law or by contract from using the information for secondary purposes beyond the purposes for which the information is shared.

1. We share information with organizations that help us process the transactions you request and protect our customers' transactions from fraud, such as sharing your credit card number with a service that screens for lost and stolen card numbers.
2. We disclose the information we collect, as described in Section 3 above, to organizations that perform services on our behalf or to other financial institutions with which we have joint service agreements i.e. a credit card clearing house. These organizations are subject to confidentiality agreements with us and other legal restrictions that prohibit using the information except to

provide the specified related services, unless you have affirmatively agreed or given your prior permission for other uses.

3. We disclose information that we in good faith believe is appropriate to cooperate in investigations of fraud or other illegal activity, or to conduct investigations of violations of acceptable use policies.
4. We disclose information in response to a subpoena, warrant, court order, levy, attachment, order of a court-appointed receiver or other comparable legal process, including subpoenas from private parties in a civil action.
5. We disclose information to your agent or legal representative (such as the holder of a power of attorney that you grant, or a guardian appointed for you)
6. We share information with third parties, in compliance with the Federal Family Educational Rights and Privacy Act of 1974 (FERPA).

### **Internet Address Information**

We use IP addresses, browser types, and access times to analyze trends, administer the site, improve site performance, gather broad demographic information for aggregate use, and to conduct investigations on fraud, illegal activity, and other violations of our Acceptable Use Policy.

### **5. Links to Other Web Sites**

Our Web sites contain links to external sites not associated with USNH e-commerce. This statement applies solely to information collected by USNH e-commerce access pages. Please be aware that USNH is not responsible for the security practices of external sites. The user is encouraged when navigating Web pages to be mindful when they depart USNH sites and to look for, and read privacy statements of each and every web site that requests personal information.

### **6. Contacting Us**

If you have questions or concerns regarding e-commerce privacy and this statement, you may direct them to [eEVENTS@maple.unh.edu](mailto:eEVENTS@maple.unh.edu)