Privacy Policy

Authorized use of customers property:

Chipheads Inc. staff and authorized sub-contractors are authorized to use computers owned by customers to the degree that such use contributes to the tasks authorized by the customers or are required to troubleshoot, examine, repair or test a computer system or other device capable of storing private or confidential data, or contributes to preventative maintenance on the computer or device. Chipheads Inc. takes no responsibility for the failure of any hardware not purchased or currently under warranty from Chipheads Inc. even if it fails while in our possession, and no responsibility for the loss or theft of any files, data, passwords or login credentials that might be stored on any hardware or given to us verbally or in writing.

Chipheads policy on customer data:

By leaving a computer system or other digital device with Chipheads Inc. staff and authorized sub-contractors, the customer gives complete and unlimited consent and unlimited access to use all data, passwords, login credentials, private or otherwise, stored on the computer system.

Chipheads staff are instructed to treat with care all customers personal information stored on computer hard drives, CDs, DVDs memory sticks, flash cards or any digital format and are prohibited from viewing, copying, discussing or distributing such data except as needed to protect data from deletion or damage, troubleshoot, examine, repair or test a device capable of storing such data or as required by state and federal law.

Chipheads policy on recycling:

Chipheads will accept NO RESPONSIBILITY for any data, files, passwords , login credentials or any kind of personal, confidential or sensitive information on any device that has been abandoned or left for recycling.

Tips for protecting sensitive data:

Customers who routinely store sensitive data on their computers or other digital devices, and are worried about who might have access to this data are advised to do the following:

1. **Change any and all passwords and login credentials after any kind of service by any computer professional or any person not 100% trusted by the computer owner and also on a regular basis.**

2. If possible, transfer all sensitive data to another device before dropping system off for service.

3. Many programs, such as Microsoft Word, have the ability to PASSWORD PROTECT sensitive files. Learn to use these features. There are also programs available that password protect picture and music files and directories. CAUTION- In the event of a hard drive crash, File Encryption can make data recovery more difficult- so always backup multiple copies of important files to separate computers or devices on a regular basis.

4. Request and read the privacy policies of any service provider you are considering hiring, such as Chipheads Inc., and make sure you understand them and that they offer adequate protection for your situation.

5. If you have sensitive or private data on your computer or other special privacy needs, consider notifying the service tech or company IN WRITING about how you would like your data handled, or request to be notified by telephone if anyone needs to view or copy certain files. Be as specific as you can about what files you are worried about.

6. Find a computer support technician or company you can trust and stick with them. Remember, the vast majority of retail computer repair and support people are honest professionals who respect your privacy and act diligently to protect it. Stick with them like you would a trusted doctor or mechani

7. If possible, request onsite service. This way you can work one on one with the tech who is working to solve your issues, and you can control what they see and don't see.


Speak with a real technician!
Minneapolis Location
612.866.8800
St. Paul Location
651.228.1942