Corfe Mullen Computers Ltd
Security & Handling of Customers Data Policy

Why?

We have a data handling policy because the data is the most important part of a computer system. It's the most important part of a computer for our clients and it's the most important part to us.

Data security means the data is not liable to loss from hardware failure, hardware theft and protected from unwanted viewing.

As part of our normal routine we store customer data in several ways:

1. We store clients computers whilst repairs are taking place even if the repair does to pertain to the computers storage devices.

2. We store client data on our own computers whilst it is being transferred between storage devices.

3. We store client data on their storage devices after a repair has taken place and the device is in the process of be disposed of.

Our experience of data security

Our experience of handling data securely is extensive. We have handled data for military contractors, for which we have signed the Official Secrets Act. We have handled data for large development companies where the intellectual property rights are of paramount concern. We have also handled data for companies who are at particular risk of cyber-attacks. Therefore, data security is an extremely important issue for us.

Storing customer computers containing data

Whilst we store a computer during the repair process and the repair does not affect the storage device e.g. PC MOT, the data is left on the device. No copies are made by us onto any other medium. The data should ideally have backup copies made and be secured by the client, before the computer is handed to us, to their own satisfaction.

If the data is secured by a password that covers the whole computer and we need this to perform the repair then we will ask for this at the start and state our intentions. The client does not have to hand over the password if they so wish. This may affect our ability to perform and/or check the repair.

The computer itself will be stored in a closable storage container within a locked building. No passwords are stored with the computer.

Whilst we are repairing a computer the data is usually handled as a 'black box'

although we may see parts of it e.g. thumbnails even though we do not intentionally look through it.

Storing client data on our own computers

There are 2 reasons why we may do this:

1. The clients storage medium is found to be unreliable e.g. the hard drive is faulty.

2. During the migration process from one computer to another.

If we find a clients data is at risk of being lost we will make every effort to retrieve it. The data will be stored on our computers while the problem is repaired. The computers are secured with password protection and are behind 2 firewalls to prevent intrusion from outside the company and from any other computer connected to our network. The data is not encrypted as this can make retaining the data more difficult. The data is handled as a 'black box'.

After the repair has been completed the data is deleted from our computers within 1 week of the completion of the repair. Periodically the free space on our computers is wiped. The data may also be scanned for virus's, spyware and any other kind of malware for ours and the clients protection.

During a migration of data between clients storage devices we may use a third computer or storage medium to facilitate this. Our copy of the client data is immediately deleted and wiped in the periodic free space wipes.

Storage of data on redundant devices

After a repair e.g. hard drive replacement, we may have storage media to be disposed of. Before it leaves our premises it will be securely wiped. If this is not possible then it will be destroyed. No client data will leave us in an uncontrolled manner.

We may reuse wiped hard drives to testing purposes. We do not use them for critical data storage because they are already considered unreliable. For this reason they will never be used in another clients computer.

Our concern for data security means we never fit used hard drives as a repair because there is too much risk of data loss due part failure.

Limitations

To manage customer expectations we must point out the limitations of our storage of data.

Nothing we do to secure client data constitutes a backup solution for use by our clients.

Computers usually come to us in a less than reliable state. This means your data may already be at risk. We will endeavour to retain the data but you are ultimately responsible for your data and if you do not have a sufficient backup solution in place before your computer fails there may be nothing we can do and we do not accept any liability for the loss of data in this situation.

We have liability insurance but where hardware can easily be replaced, data cannot.