BEST PRACTICE #6

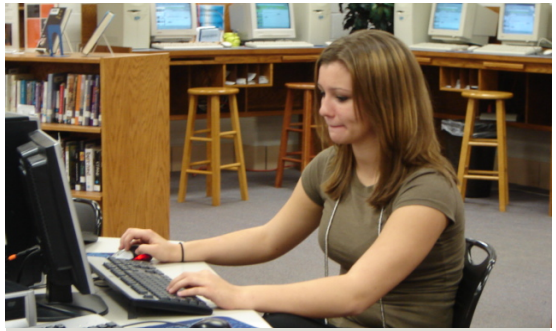
LEARN WHAT DATA IS "CONFIDENTIAL"

Sensitive and Personal Data

- Social Security Numbers*
- Date of Birth
- Bank Account*
- Credit card number*
- Debit card number + access code*
- Driver's license or non-driver ID*
- Wage information
- Giving / donation information
- Academic Information
- Employee phone number

* Defined by New York State Breach Law

Security is *everyone's* business.



DATA INTEGRITY

Shared Data

Data drives many of the operations and decisions at the College.

The data is also used in reporting to government, accrediting and other regulatory agencies.

Our College profile and government funding depend on it.

Most administrative offices share the same data.

Data Accuracy

If you are not sure about a field or a value, ask.

NAZARETH COLLEGE INFORMATION SECURITY GROUP
isg@naz.edu

Nazareth College

INFORMATION SECURITY GROUP

Data Security Six Best Practices

Six simple practices to protect the College's confidential information.

NAZARETH COLLEGE EMPLOYEE BEST PRACTICES

BEST PRACTICE #1

DATA HANDLING

Do not discard lists with confidential information into the trash—shred them.

Do not permanently store 16-digit credit card information anywhere. Shred paper records.

If you need to send data to an agency, ITS can help with encrypting the transmission.

Do not send confidential information in plain text e-mails, or as un-encrypted attachments. It is not safe. ITS can help.

BEST PRACTICE #2

DATA STORAGE AND SHARING

No confidential information should be permanently stored on your desktop, laptop or removable device, unless you have obtained permission and the file is *encrypted* and *password protected.*

Do not transmit confidential information to outside parties, unless you have obtained permission and are using a secured method of transmission.

BEST PRACTICE #3

AT YOUR DESK

Stepping away from your desk for a few minutes?

Turn off your monitor.

Lock your computer <control + alt + delete> or log off.

Turn papers with information face down on your desk.

General Workstation Safe Practices
Lock your desk when you are not there.

Keep folders with confidential information in locked file cabinets.

Do not leave reports in the printer.

BEST PRACTICE #4

CREDIT CARD, CASH, CHECK

Think about confidential information as if it were cash.

Do not leave checks out in the open.

Do not leave credit card transaction information on your desk – put away immediately.

BEST PRACTICE #5

PASSWORDS

NO ONE should know your password. Treat it as you would your house key.

Passwords should be changed every 90 days

Passwords should not be transmitted over the internet by email or any form of communication, unless they are encrypted.

Passwords should be at least 8 characters long, with a combination of upper and lower case alpha, numeric and special characters. Do not use dictionary words.

Passwords should never be written down.