Restricted Data The following restricted data has been determinde by the Data Custodians (institutional owners of the data) or because it is covered under Federal Law, State law, or by University Policy	
Institutional or Personal Financial Data Such as:	Credit Card Numbers, P-Card Numbers, accounts receivable transaction records, Donor gift history including dates and amounts, Institutional checking or investment numbers
Employee Data Such as:	benefits information, birth date, banking information, Health Insurance Policy ID Numbers, Transcripts, education records
Personally Identifiable Data Such as:	Passport and visa numbers, Social Security Numbers
State or Federally Protected Data such as:	law enforcement records, Health or medical Information, including Protected Health Information (PHI), Information exempted in Florida Statute 119,Export controlled information under U.S. laws, HIPAA protected data, FERPA protected data, Gramm-Leach-Bliley
University Data Such as:	Responses to Bids/RFPs/ITNs until 30 days after award, Privileged attorney-client communications, Computer account passwords
Student Data Such as:	Student Banking Information, Transcripts, Student Payment History and Bills, Admission applications, education records, financial Aid and Scholarship information, registration information, judicial student affairs, Grades with UIN's and Student Names

Click on above image for larger view

What Is Restricted Data?
Restricted data is data that are subject to specific protections under federal or state law or regulations or under applicable contracts, whose loss or unauthorized disclosure would impair the functions of the University, cause significant financial or reputational loss or lead to potential legal liability.

How Do I Handel Restricted Data At Work:
It is okay for you to work with this data, but you have to be mindful of where you store it
Electronic Copies:

- Your own departments file share
- If stored on your local computer or laptop, the data must be encrypted
- Remove it when you no longer need it

Physical/Hard copies:

- Should be printed locally so no one can grab it before you can
- Must be retrieved immediately if no local printer available
- Do not fax it to anyone as you cannot verify they got it
- Store in a secure location, such as a locked cabinet
- Dispose via a paper shredder

How do I Handle Restricted Data at Home:

- Remote access to the data must be done via FGCU's VPN services unless you use systems such as Gulfline or Canvas. These systems use a secured connection (SSL) and require authentication – Click here for more information on connecting remotely
- It is strongly advised to not download restricted data to your remote computing device
- If downloaded, it must be encrypted –Link to BTS site explaining encryption
- Remove it when you no longer need it

What is Encryption and Why Use It?
Encryption is the method of using a user supplied key, such as a password, to encode a file into an obfuscated format. This makes the file unusable until it is decrypted back into its original format. To do so, you have to use the key and the program that were used to encrypt the file. Since the file will be unusable without the encryption key, it is imperative that you use a key that you can remember.

Can I send Restricted Data to Others?

- Must not be sent via email
- May be shared with other people at FGCU using your departmental share or the cross department share
- If you must send the data to someone outside the university, it must be encrypted and sent via secure method if possible

I'm Using Restricted Data on my home PC, What Should I Do?

- Determine if you MUST save the restricted data.
- If you Must store restricted data on you PC then I MUST be encrypted.

How do I Encrypt Files?

- Business Technology suggests using a program called 7zip to assist users with encryption and both Windows and Mac operating systems. Detailed instructions for how to encrypt/decrypt a file can be found on the Business Technology Services web site. – Link to BTS site explaining encryption

How Do I Dispose Equipment that has stored Restricted Data

- Devices such as desktop computers, laptops, printers, tablets must be disposed of by one of the technology departments at FGCU to prevent restricted data from leaving the university
- Other storage devices, such as CDs, flash drives, tapes must be disposed of via the office of Records Management

Where Can I Store Restricted data?
If you need to store restricted data in electronics format, FGCU recommends you do so in your departmental share folder, or cross group folder. If you store the electronic data anywhere else, such as your FGCU computer, or home computer you must make sure the data is encrypt.

What about Cloud Storage, or Flash Drives?
Other storage locations, such as cloud storage, or removable drives should not be used for restricted data. If this location is the only available location restricted data stored there has to be encrypted. Does the policy say this?

I May Have Lost Some Data. What Do I Do?
In the case of loss of restricted, please contact the FGCU Helpdesk immediately.at 239-590-1188.

How Long Can I Store Restricted Data?
You should remove restricted data from any system that is not the permanent resting place of the data as soon as possible. Please consult the office of Records Management with any questions you may have regarding storage, document management, security, retention and destruction.