



The
Baptist College
of Florida

"Changing the World Through the Unchanging WordSM"

Student Computing Guide

Graceville Campus



Information Technology

Published: January 28, 2011

This document can be accessed on the internet at:

http://www.baptistcollege.edu/IT/media/Student_computing_guide_gville.pdf

Contents

Introduction	2
Feedback.....	2
Support	2
Support for Personally Owned Equipment	2
Computer & Information Systems Policy.....	2
Copyrights, Trademarks and Intellectual Property	2
Authorized Student Computer Account	3
The password	3
MyBCF	4
Browser Compatibility.....	4
Using MyBCF	4
Email Guide.....	5
Unsolicited Commercial Email – SPAM and Suspicious Email.....	5
Accessing Email	5
Outlook Web Application	5
Configuring a Mobile Device or Smart Phone (iPhone, Blackberry, etc.)	5
Configuring an Exchange Client such as Outlook (2007 or later)	5
Setting up a POP3 Mail Reader	5
BCF Student Access Computer Locations.....	6
Student Network Drives.....	6
Printing & Making Copies	6
BCF Wireless	7
Tips, FAQs, and Troubleshooting:.....	7
Tips:	7
Troubleshooting:	7
FAQs:.....	8
Security of wireless networking	8
bcf wireless secured	8
College Policy concerning 2.4 GHz Devices and personal networking on the Graceville Campus	9
Configuring software that requires a “Socks 5” proxy server (an example is Skype)	9
Instant Messaging Clients	9
Internet content filter.....	10
Internet file downloads.....	10
Computer Security and Safety.....	11
Virus Protection and Firewall.....	11
System Updates	11
Online Safety and Privacy	11

Introduction

Welcome to The Baptist College of Florida!

Information Technology (IT) has developed this guide to provide new and returning students with information needed to utilize the College's Information Systems.

The Baptist College of Florida provides Information Systems to meet operational, financial, and academic needs. These resources are valuable, and their abuse can have a far-reaching negative impact. IT is responsible for balancing the need for security with practical application.

The mission statement for the Information Technology (IT) department includes the charge to facilitate computing services that allow BCF to accomplish its mission of educating and training ministers and other religious workers. As such, it may not be appropriate to support all the technology services that are available in a home use environment on the Graceville campus.

Feedback

Questions, comments, and recommendations can be submitted to IT@baptistcollege.edu.

Support

IT provides and supports the data systems and network resources that make up the College's Information Systems. IT supports faculty, staff, students, prospects and alumni as they use college resources.

Support for Personally Owned Equipment

IT does not provide support for systems owned by individuals. The Baptist College of Florida's Computer and Information Systems Policy does not allow IT to support student owned computers or computer related equipment.

Computer & Information Systems Policy

The BCF Computer and Information Systems Policy (CISP) governs all of the College's computers and information systems. This policy can be found in the student handbook and is accessible online at

<http://www.baptistcollege.edu/IT/media/CISP.pdf>.

At the direction of the Senior Vice President, IT conducts random audits to ensure compliance with the Computer and Information Systems Policy.

Copyrights, Trademarks and Intellectual Property

Do not violate the copyright, trade secret, patent or other intellectual property rights of any person or company. Do not install or distribute software products that are not appropriately licensed. Do not make unauthorized copies of copyrighted material.

Authorized Student Computer Account

In accordance with the BCF Computer and Information Systems Policy, each student is issued an authorized computer account. This account may be used only in accordance with its authorized purposes. You are responsible for safeguarding your own authorized account, specifically the user name (IDNumber) and password. All students are solely responsible for all activity on or associated with their account.

After the appropriate account has been created, you are authorized to use your account for the following purposes:

- Logging in to The Baptist College of Florida's online campus, MyBCF <https://mybcf.baptistcollege.edu>
- Baptist College email for academic and personal non-commercial purposes. The email account will be created at the beginning of the semester for which you are admitted or re-admitted. ^{*see note below}
- Wireless network use for academic and personal non-commercial purposes. ^{*see note below}
- Computer Lab and Library computer use for academic purposes. ^{*see note below}
- Limited printing in the Computer Lab, Music Labs & Library for academic purposes. ^{*see note below}

***Please note:** Baptist College email accounts and network logon accounts will be created **at the beginning of the semester for which you are admitted or re-admitted**. It will remain active as long as you remain a current BCF student not subject to the BCF readmissions policy.

Students are authorized to connect a notebook, desktop or handheld computer to the wireless network after the network logon account has been created. No other type of connection is authorized. Students may not connect or allow the connection of any other devices to any BCF Information System.

The password

Your user name (IDNumber) and password is the entry point to BCF Information Systems. The password is sent to you by the IT department. This same user name and password will be used for accessing MyBCF, college email, the Graceville campus wireless network, and student-access computers and printers.

All network activity is logged by user name where applicable; any activity shown as associated with a particular user name is the responsibility of that user, regardless of who is actually using the account. Do not allow others to use your account.

Keep your password secure to ensure all activity is logged to the correct user.

General guidelines for keeping your password secure are:

1. Do not save your password in your internet browser or in any other software.
2. Do not ask anyone else for his or her password. Do not share your password with anyone.
3. No password should be spoken, written, e-mailed, hinted at, shared, or in any way made known to another.
4. No password should be displayed or concealed on or near your computer workspace.

If you believe someone else may know your password notify IT immediately, and a new password will be issued.

No one from the BCF IT department will request your password over the telephone or through any email message. Do not give out this information.

MyBCF

MyBCF is our online campus. MyBCF is the website that allows you to register for classes, check your grades, view campus groups, edit personal College information, and access online portions of courses.

The website is <https://mybcf.baptistcollege.edu>.

Browser Compatibility

The browsers that are supported for use with this application are:

- Internet Explorer 7.0 and 8.0 for Windows XP, Vista, Windows 7
- Firefox 2.0.0.20 for Windows XP, Mac OS X (Version 10.2 or 10.4)
- Firefox 3.0.7 and 3.5.x for Windows XP, Mac OS X (Version 10.4)
- Safari 3.2.1 for Mac OS X (Version 10.4.11)

Versions later or earlier than these may or may not work properly.

Note: Java and JavaScript must be allowed, or enabled, in the browser's configuration. Popups must be allowed from this website as well.

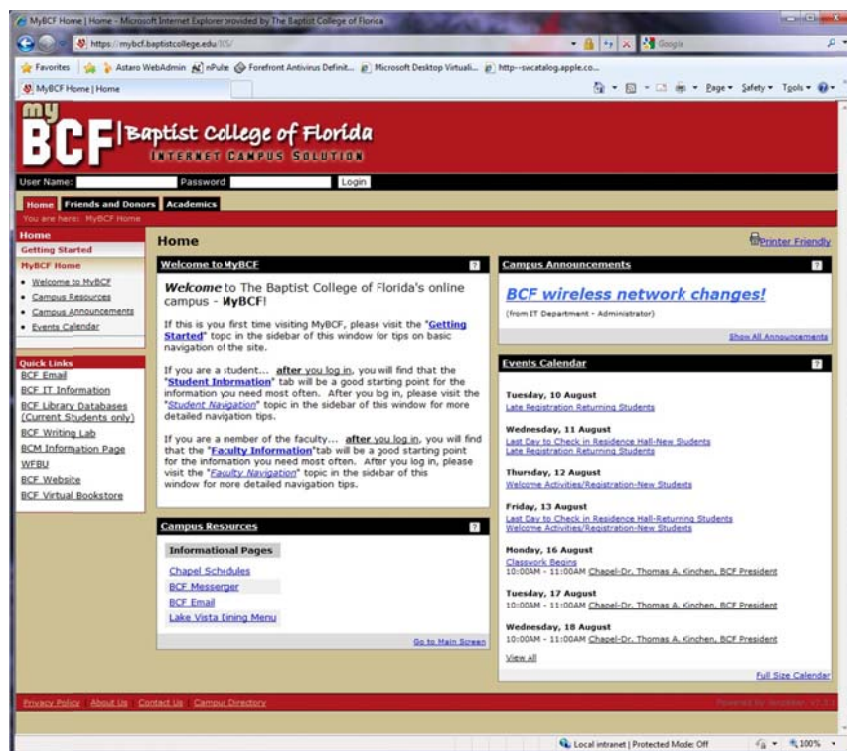
*** The above does NOT apply to using BCF's wireless service, only to the website <https://mybcf.baptistcollege.edu>***

Using MyBCF

Your "User Name" for MyBCF is your ID number; the password is the one sent to you from the IT department.

Check out the "Getting Started" and "Student Navigation" topics on the left sidebar of the home page for tips about using MyBCF after you log in.

The following is an example snapshot of the login page for MyBCF:



Email Guide

Students will be assigned a baptistcollege.edu email address. This email address will be used for college correspondence. **Your email account will be created at the beginning of the first semester for which you are admitted or re-admitted.** It will remain active as long as you remain a current BCF student not subject to the BCF readmissions policy.

Unsolicited Commercial Email – SPAM and Suspicious Email

The College employs several levels of spam prevention including Microsoft Intelligent Message Filter, Microsoft Forefront antivirus and spam filtering, real-time block lists, reverse DNS lookups, and Astaro spam filtering.

If you receive spam in your mailbox, add the sender to the *Blocked Senders List* in Outlook Web Application or your email client; then delete the spam message. *Periodically, check your junk email folder for messages that may have been marked incorrectly.*

Resources:

Best practices: <http://office.microsoft.com/en-us/outlook-help/best-practices-to-help-prevent-spam-HA001119422.aspx>

Toward a Spam-Free Future: <http://www.microsoft.com/mscorp/execmail/2003/06-24antispam.msp>

How to handle suspicious email: <http://www.microsoft.com/protect/fraud/spam/email.aspx>

Accessing Email

There are several methods to check your email. You may check it using a web browser. You may set up an email client such as Outlook. If the email client has an exchange option, use the exchange option. You may also use POP or IMAP to access your email.

Outlook Web Application

Check your student email online by visiting: <https://mail.baptistcollege.edu>

Mobile devices like cell phones and handhelds can access a mobile version at <https://mail.baptistcollege.edu/oma>

Your user name is your IDNumber and the password is the one sent to you by the IT department.

Configuring a Mobile Device or Smart Phone (iPhone, Blackberry, etc.)

For newer versions of the smart phones and PDAs, specify the account type as “**Exchange**” and provide your email address and password. The user name is your “**IDNumber**”. Some devices may require “**IDNumber@bcf.edu**”. The server name is “**mail.baptistcollege.edu**”. On some devices, it may require the Outlook Web Access address which is “**https://mail.baptistcollege.edu**”. If a domain name is required, it is “**bcf.edu**”.

Configuring an Exchange Client such as Outlook (2007 or later)

Specify the account type as “**Exchange**” and provide your email address and password. Your user name is your “**IDNumber@bcf.edu**”. The server name is “**mail.baptistcollege.edu**”.

Setting up a POP3 Mail Reader

The email account type is **POP3**. The incoming and outgoing mail server name is “**mail.baptistcollege.edu**”. Your “User Name” or login for the *Incoming mail server* is in the format of “**IDNumber@bcf.edu**”. Your “User Name” or login for the *Outgoing mail server* is in the format of “**IDNumber**”. Use your **password** for *both* the Incoming and Outgoing mail server.

BCF Student Access Computer Locations

Computers are available for students to use in the Computer Lab and the Library on the Graceville campus.

You must use your BCF network logon account to use the student access computers on the Graceville campus.

This logon account will be created at the beginning of the first semester for which you are admitted or re-admitted. It will remain active as long as you remain a current BCF student not subject to the BCF readmissions policy.

This will be the same user ID and password that are used to access MyBCF and BCF email.

The Computer Lab and the Library may have additional rules governing the use of these computers.

Music students are also permitted to use the computers in the Music Lab.

Students are prohibited from using any other college-owned computers, including those in the classrooms and offices.

Student Network Drives

These are available only on BCF Student Access Computers on Graceville Campus.

Save all files to the "U:" drive when using Computer Lab or Library Computers.

(Access the "U:" drive by opening "My Computer.")

Printing & Making Copies

Student printing is available only on BCF Student Access Computers.

The only copier designated for student use is available in the Ida J. McMillan Library in Carlton Hall.

Students may print one copy of a document. Additional copies should then be made using the publicly accessible copier/printer located in the Library. Students may not use copier function without paying for the copies.

The printers located in the Computer Lab, Music Lab and the Library are for academic purposes only.

These printers may **not** be used for personal, ministerial, or commercial purposes.

Students are prohibited from using any other college-owned printers/copiers.

Arrangements should be made with the professor if a student needs a class set of a document.

BCF Wireless

The Baptist College of Florida operates a wireless internet access service, available throughout most areas of the Graceville Campus. The wireless service is available for use by current students, alumni, faculty, and staff. ^{*see note below}

To use the service, an 802.11b/g (Wi-Fi) card or device is required. Most notebooks, PDAs, handheld PCs, and some desktop computers come with wireless connectivity. If one does not come with a wireless card, usually an 802.11b/g wireless adapter can be added. Contact your hardware manufacturer for more details about your specific device.

The wireless network name (or SSID) is **bcf wireless**- connect to this network. The first time you open a browser after connecting, you should be redirected to the login web page. Provide your user name (IDNumber) and password.

***Please Note: Your network logon account will be created at the beginning of the first semester for which you are admitted or re-admitted.** It will remain active as long as you remain a current BCF student not subject to the BCF readmissions policy.

Tips, FAQs, and Troubleshooting:

Tips:

- If you are not redirected to the login web page when you open a browser, make sure:
 - That **no** proxy servers are configured, and that the 'auto-detect' of proxy settings is **off**.
 - Your browser is configured to open **one** web page when it starts.
 - If you are using a security suite, make sure it recognizes the page's certificate as valid.
 - ✓ General information for doing this can be found at:
http://wireless.baptistcollege.edu:81/login_cert.html
 - A few security and accountability applications, such as "Covenant Eyes®" require contact with the company's servers before allowing internet browsing – in these cases, you will need to configure and use a wireless profile to connect to "bcf wireless secured". General information for that is listed on the next page. Detailed instructions are available at:
http://help.wireless.baptistcollege.edu/bcf_wireless_secured.html
- Some applications, such as Skype®, may require configuring a "Socks 5" proxy server.
 - The proxy settings are server "10.1.28.1" and port "1080".
 - You will need to login to "bcf wireless" using the login web page **before** using the application.

Troubleshooting:

- If you see a certificate error instead of the login page:
 - ✓ Make sure that the root certificate for this page has been installed. Instructions for doing this can be found at: http://wireless.baptistcollege.edu:81/login_cert.html
- If no page is displayed, and the browser seems to "hang" or "freeze":
 - ✓ Some poorly designed browser add-ins and toolbars will prevent any page from loading until the add-in or toolbar "checks in" with a home server. These problem add-ons should be disabled or removed – they will prevent the login page from being displayed.
 - ✓ Some security and accountability software prevent browsing before the software is able to contact the company's servers. In this case, use the "**bcf wireless secured**" network. Information for connecting to that network are listed on the next page.
- If an "App" on a mobile device, a "Desktop Gadget", or "Widget" is not working:
 - ✓ Any application that uses an internet connection will only work after you have used a browser to login to "bcf wireless." Examples are "Apps" on handheld devices that retrieve weather reports or stock prices. There is also the option of using the "**bcf wireless secured**" network.
 - ✓ For these to work on "bcf wireless", first open the internet browser and provide your login information. You may then close the browser, doing so will not disconnect your login session. After logging in, all the various applications on the device or computer will be able to access their internet services using your wireless session.

FAQs:

- Q: What is my username and password for the wireless network?
 - If you are a current student, login with the same user name and password that you use for MyBCF.
 - If you are a new student or a re-admitted student, then you will be not be able to use the wireless network until the beginning of your first semester for which you are admitted or re-admitted.
- Q: What is session-status link on the welcome page used for?
 - This will allow you to quickly log out of the wireless network, and to view stats for the session.
- Q: Can I register for a static IP/hostname?
 - No. Only dynamically assigned IP addresses are supported.
- Q: My reception seems poor and sometimes drops off.
 - If you have problems with reception, try moving the computer or wireless adapter. An external antenna has been shown to improve reception in some areas of the Graceville campus.
- Q: Who do I call for support?
 - Notify the IT department of wireless network problems by calling 850.263.9081, 850.263.9058, or 850.263.9020
 - **Please Note:** The Baptist College of Florida and the IT Department will not support computer equipment or software that is not owned by the college. IT does not provide technical support for student owned equipment. It will be the sole responsibility of the student to install and configure his or her personally owned devices and software.
 - Send questions or comments regarding the wireless service to IT@baptistcollege.edu.

Security of wireless networking

Wireless networking is inherently insecure. Any traffic on a wireless network can be intercepted and easily read if it is unencrypted. For this reason, it is very important to use Secure Socket Layer (SSL) when connecting to sites or service that request or contain private or confidential information.

To provide additional protection for those who desire to use it, and those that use security or accountability applications, such as "Covenant Eyes®", that require authenticating to the network before using any browser, the Baptist College of Florida also operates a wireless network that uses WPA-Enterprise encryption. This encrypts **all** wireless traffic, not just those sites that use SSL.

bcf wireless secured

This network's name (SSID) is "**bcf wireless secured**".** It uses WPA-Enterprise encryption and 802.1x user authentication for access control. If you do decide to take advantage of this network, you will need to set up and configure a wireless profile to do so. **Please Note:** *Switching from "bcf wireless" to "bcf wireless secured" or back again will require logging out and disconnecting, and then a waiting period of approximately 1 hour before attempting to connect to the other network.*

The method of configuring a profile is specific to the computer or device being used. Following are the general points of information needed:

- For most computers and devices, manually create a wireless profile.
- When prompted, use "**bcf wireless secured**" for the network name (the SSID.)
- For Windows® operating systems:
 - ✓ Turn **off** the option to "Validate server certificate".
 - ✓ Turn **on** the "Enable Fast Reconnect" option.
 - ✓ Change the "Specify authentication mode" option to "**User Authentication**".
 - ✓ Make sure that the option to automatically log in with the "Windows username and password" is **disabled**.
 - ✓ To keep your password secure, turn off any option that will remember your credentials.
- When you connect to this network, you will be prompted to enter your user name and password as you connect. (There will be no browser page login.)
- Step-by-step instructions for connecting to this network are available from the IT department on request.

College Policy concerning 2.4 GHz Devices and personal networking on the Graceville Campus

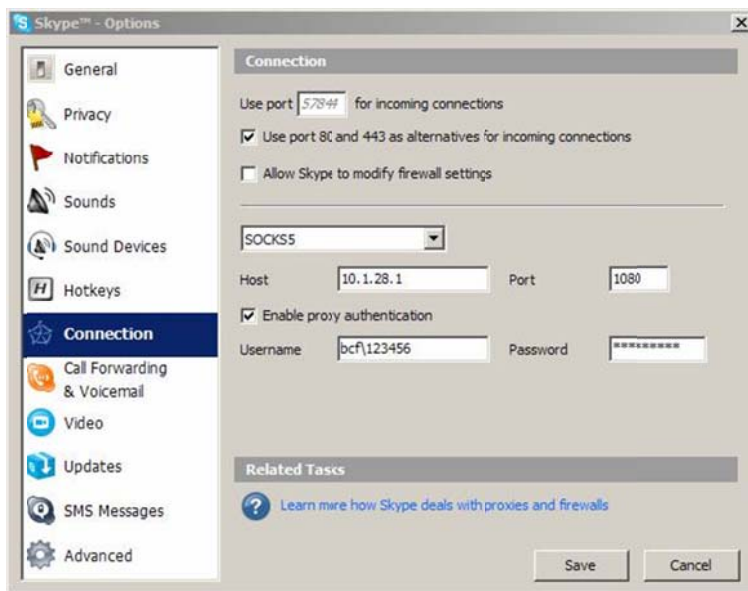
Personally owned wireless access points, wireless routers, Base Stations, and peer-to-peer (or ad-hoc) networks should **NOT** be operated anywhere on the Graceville campus. This interferes with others who need to use the wireless service that is operated by the college.

Those who violate this policy will be referred to Student Services. If you know of someone who is violating this policy by operating a wireless service on campus, please report this to Student Services.

The wireless networks operated by The Baptist College of Florida on the Graceville campus rely on the 2.4 GHz frequency band, and will soon expand to use the 5.8 GHz frequency band as well. Many devices can cause interference. These devices include cordless phones, wireless video monitors, and any other devices that operate on 2.4 GHz. These devices should **not** be operated on the Graceville campus due to the interference they cause.

Configuring software that requires a “Socks 5” proxy server (an example is Skype)

- Specify a proxy server of 10.1.28.1
- Specify port 1080.
- Enable proxy authentication.
- Type your username (ID Number) and your password in the spaces provided.



Instant Messaging Clients

We cannot guarantee that any specific client-based instant messaging software will work.

However, the use of web-based instant messaging software that use AIM, MSN, and Yahoo services is supported.

In research, we found several web sites that can be used for this: www.meebo.com, www.koolim.com, and www.iloveim.com.

Internet content filter

Most web sites are categorized, and websites that meet certain criteria will be blocked and logged. For example, all websites categorized as pornography will be blocked. If you visit a website that matches these criteria, you will see a screen such as this.



If you feel that a website is incorrectly categorized, please **e-mail the website's URL** to the IT Department (it@baptistcollege.edu) so we can investigate the issue.

Internet file downloads

For your protection and the protection of the college's network, all web-based content will be scanned for viruses and spyware. When you download a file, you will see a screen like this.



After the firewall downloads the content, the firewall will then scan the content for viruses. If the file is clean, a screen will be presented that will prompt you to download the file to your computer. However, if the file is infected you will be presented with a screen that gives you information on the virus it detected, and you will not be able to download the file to your computer.

The mission statement for the Information Technology (IT) department includes the charge to facilitate computing services that allow BCF to accomplish its mission of educating and training ministers and other religious workers. **As such, it may not be appropriate to support all the technology services that are available in a home use environment on the Graceville campus.**

Computer Security and Safety

Virus Protection and Firewall

You should run firewall software on any computer connecting to any wireless network. Microsoft Windows and Mac OS X both have built-in firewalls. Computers must be running virus protection with a virus pattern that is no more than 30 days old to be reasonably protected from malware. It is best to update the virus pattern or virus definitions every day.

Several anti-malware and general computer security resources are listed below for your convenience. The Baptist College of Florida makes no guarantee as to the quality or effectiveness of these products.

No-charge solutions examples:

Microsoft

http://www.microsoft.com/security_essentials/ (Free for home users.)

AVG Anti-Virus

<http://free.avg.com/us-en/download-avg-anti-virus-free> (There is a "Free Edition".)

Avast! Anti-Virus

<http://www.avast.com/free-antivirus-download> (Free of charge for home users or non-commercial use.)

Spybot Search & Destroy

<http://www.safer-networking.org/en/download/index.html>

OpenDNS – a web content filtering and security solution

<http://www.opendns.com> (There is a free version.)

Subscription-based solutions examples:

ESET (NOD32 antivirus)

<http://www.eset.com/>

Trend Micro

<http://us.trendmicro.com/us/home/>

Panda Software

<http://www.pandasoftware.com/>

Computer Associates

<http://store.ca.com>

McAfee

<http://mcafee.com/us/>

Norton/Symantec

<http://www.symantec.com/norton/index.jsp>

System Updates

Regularly install security patches on your computer operating system.

Microsoft Windows

Windows Update Information: <http://www.microsoft.com/windows/downloads/windowsupdate/automaticupdate.msp>

Mac OS X

Get the Latest Security Updates for Mac OS X: <http://www.apple.com/support/>

Online Safety and Privacy

Please take the time to educate yourself about computer online safety. There are many excellent resources available to you concerning this topic. Following is a link to online safety and privacy information on Microsoft's site:

<http://www.microsoft.com/protect/default.aspx>.

Microsoft Security help and support is available for the home user to help you obtain support for security-related issues such as viruses and security updates. http://support.microsoft.com/contactus/cu_sc_virsec_master?ws=support