Partnership FOR CHILDREN
OF CUMBERLAND COUNTY

Facility & Tenant Committee
Meeting Agenda

Quorum = 3 (33%) (Total Committee Members = 6)

Monday, April 20, 2026
11:30 am – 12:30 pm
Hybrid Meeting
Please sign in via the CHAT room for ZOOM attendance

Be the Driving Force . . .

I. Determination of Quorum & Call to Order – Joe Deaton, Chair

II. Approval of Minutes – February 16, 2026*

III. Lease Approvals and Renewals*
A. Applicants- None
B. Full Circle Therapeutic Services- Suite 406- Exp 5/31/2026- YES
C. Delmar Counseling Ser- Suite 350- Exp 6/30/2026-
D. Living Well Counseling PLLC- Suite 411 Rm 2406, 2407- Exp 6/30/2026- YES
E. Outward Solutions, PLLC- Suite 418- Exp 6/30/2026- YES

IV. IT Report*
A. Password policy
B. Cyber Security Training
C. Data Retention
D. Data Backups

V. Keycard Access* - Prohibit tenants from entering on closed days and emergency shutting down

VI. Phase III Window Project[Δ]**-** Update

VII. Space availability report [Δ]

VIII. Sustainability Workgroup Report [Δ]

IX. Information
A. Next scheduled meeting: Monday, May 18, 2026, from 11:30 a.m. – 12:30 p.m.

X. Adjournment – Joe Deaton, Chair

* Needs Action [Δ] Information Only ***!*** Possible Conflict of Interest (Recusals)

[e] Electronic Copy (Hard copies are available upon request)

351 Wagoner Dr. • Suite 200 • Fayetteville, NC • 28303
(910) 867-9700 • Fax (910) 867-7772
www.ccpfc.org

NC Pre-K a partner in the Be the Driving Force.

Partnership for Children of Cumberland County, Inc. (PFC)
Hybrid Facility & Tenant Committee Meeting Minutes
February 16, 2026 (11:30 a.m. – 12:02 p.m.)
Be the Driving Force

MEMBERS PRESENT: V-Al Brunson, IP-Joe Deaton, IP-John Bantsolas, IP Martin Swinney
MEMBERS ABSENT: Haja Jallow-Konrat, Ebone Williams
NON-VOTING ATTENDEES: IP Mary Sonnenberg, IP-Marie Lilly, IP- Karen Staab, IP- Kesia Wilson, IP-Michelle Downey, IP-Mike Yeager, IP- Jeremy Julch, IP-Carolin Hardy
IP-Attended in person, V- Attended Virtually

AGENDA ITEM	DISCUSSION & RECOMMENDATION	ACTION	FOLLOW-UP
I. Determination of Quorum & Call to Order – Joe Deaton – Committee Chair	The hybrid meeting of the Facility & Tenant Committee was held on Monday, February 16, 2026, beginning at 11:30 a.m. pursuant to prior written notice to each committee member. Joe Deaton – Committee Chair, determined that a quorum was present and called the meeting to order. Carolin Hardy was the Secretary for the meeting and recorded the minutes.	Called to Order	None
II. Introduction of Martin Swinney	Mr. Swinney stated that he relocated to the area in July and has been residing locally for approximately six to seven months. He previously served as a Chief Information Officer for a healthcare consulting company and held director-level roles supporting several hospitals, with approximately twenty years of experience in the healthcare and information technology fields.	None	None
III. Approval of Minutes A. January 12, 2026*	The January 12, 2026, minutes were previously distributed electronically to committee members for review. Marie Lilly requested a correction to be made to the minutes so that they reflect "hybrid" instead of "virtual" The chair asked for a motion to approve the minutes with the correction reflecting "hybrid." John Bantsolas moved to accept the meeting minutes as changed. Al Brunson seconded the motion. The motion carried.	Motion Carried	None
IV. Lease Approvals and Renewals* A. Applicants: None B. Selfly Enterprise, PLLC - Suite 333- Exp 04/30/2026- YES C. Beautifully Woven Counseling and Consulting Services- Suite 311- Exp 05/31/2026-YES	A. Applicants: None B. Selfly Enterprise, PLLC - Suite 333- Exp 04/30/2026- YES C. Beautifully Woven Counseling and Consulting Services- Suite 311- Exp 05/31/2026-YES Both the above tenants expressed clear interest in remaining at the facility. Staff recommends approval of fitness for tenancy and authorization for Michelle to negotiate new lease agreements for both tenants. Al Brunson moved to approve the staff recommendation to renew the leases for Selfly Enterprise, PLLC and Beautifully Woven Counseling and Consulting Services, and to authorize approval of new lease agreements. John Bantsolas seconded the motion. The motion carried.	Motion Carried	Take to Board of Directors for Approval

V. Phase III Window Project-Update$^{\Delta}$	Provided by Mike Yeager: • Both the front and side window sections have been completed, including installation of the rooftop soffit trim, which was finished late Friday afternoon. The Committee was informed that installation of the remaining two to three windows is pending due to a measurement issue identified during installation. These windows were reordered and are expected to arrive on Thursday. Once installed, the contractor will coordinate with the roofing company to place the cap, which will bring the project close to completion. Mr. Yeager also shared that a price proposal has been requested for a change order to install a protective wall backer along the 300-side corridor in areas where chairs have caused damage. Rather than a traditional chair rail, a flat backer will be installed to protect the walls while allowing chairs to remain closer to the wall. The backer will be painted to match the existing wall color using latex trim paint. • Additional change orders are currently in progress. These include the installation of mounting brackets at the top of the C section, as required by the project engineer, and corrective work to the trim cap after it was determined that the original metal gauge was insufficient. The contractor has reinforced and leveled the trim cap in accordance with engineering recommendations. Final approval of these change orders is pending review by the engineer. • It was reported that despite recent snow and rain events, no water intrusion or performance issues have been observed at this time. The windows are covered under a five-year warranty, and staff were encouraged to report any concerns immediately. Phase II warranty-related work remains ongoing, with plans for the contractor to install custom semicircle flashing to address remaining issues.	None	None
VI. Space Availability Report$^{\Delta}$	Provided by Mike Yeager: • Approximately 4,030 square feet of space is currently available for lease. This includes the remaining portion of Suite 411 (1,533 sq. ft.), Suite 165 (867 sq. ft.), Suite 130 (964 sq. ft.), and Suite 326 (374 sq. ft.). Marketing for Suite 130 has been on hold while Phase III construction is completed and will begin once that work wraps up. Space previously occupied by 4C includes three rooms that have already generated interest from existing tenants. If pursued, these would be handled through lease amendments. • Current occupancy was reported at 88.4%, with 50% occupied by the Partnership for Children and nonprofit tenants and 38.4% by for-profit tenants, leaving 11.6% of the building unoccupied. • Marketing efforts were discussed and currently consist primarily of word of mouth, exterior signage with QR code access, and occasional social media posts. The possibility of using a third-party marketing agency was briefly discussed; no action was taken.	None	None

VII. Sustainability Workgroup Report[Δ]	Provided by Mike Yeager: • Considerations related to facility funding and long-term planning are taking place. It was clarified that if the building were sold within five years of project completion (anticipated around March), repayment of the $250,000 CDBG grant would be prorated by year. There is no repayment requirement associated with the Cannon Foundation funding, as this was clarified at the time the grant was awarded. These factors were noted as part of broader decision-making considerations. • Deferred maintenance needs are beginning to surface. While the building is not new, upcoming major considerations include the roof and elevators. Elevator replacement is not planned unless one becomes non-operational, though estimated costs for both elevators and roof replacement have been identified for future planning • Committee discussion also touched on staff perspectives and space needs. Leadership noted that staff are aware the organization is evaluating options, though no decisions have been made. Regardless of ownership outcomes, the organization expects to reduce its footprint due to changes in staffing levels and the conclusion of certain Region 5 contracts. Current staffing stands at approximately 41, down from prior levels of 55–60. • Leadership explained that reducing space usage—particularly on the first floor of Tower 1, is being actively considered, as leasing available space generates program income that supports operations. Staff will continue to be kept informed as discussions progress, and leadership will review space needs as part of ongoing planning.	None	None
VIII. NCPC Basic Cybersecurity Framework Assessment Report[Δ]	Provided by Mary Sonnenberg and Jeremy Julch: • The Partnership continues to experience scam and phishing emails. Cybersecurity insurance was obtained when Family Connects began due to increased data sensitivity, and systems remain segmented so that health-related data is accessible only to authorized staff. • Multi-factor authentication was implemented approximately two years ago and remains in place. Upon renewal, cybersecurity coverage was reviewed and ultimately added as an endorsement to the organization's Erie insurance policy, resulting in cost savings and improved coverage. • The North Carolina Partnership recently completed cybersecurity assessments for all local partnerships. While the organization was found to be in relatively good standing, areas for improvement were identified, including IT planning, staff training, and governance processes. A recent phishing test was conducted, and additional staff training will follow. • Governance expectations were discussed, including recommendations for regular cybersecurity review at the senior leadership level, with relevant updates brought forward to the Committee as appropriate. Staff noted that cybersecurity policies are	None	None

	currently being updated to align with NCPC guidance and will be presented first to leadership, then to the Committee, and ultimately to the Board for approval. • The Committee discussed the importance of communication with tenants regarding cybersecurity, particularly related to electronic rent payments and potential scam emails requesting payment changes. Staff agreed it would be beneficial to notify tenants and share basic guidance, and to explore holding a tenant meeting or distributing written information.		
IX. Information	The next meeting will be held on Monday, March 16, 2026 at 11:30 a.m. – 12:30 p.m.	None	None
X. Adjournment – Joe Deaton – Committee Chair	As there was no further business to discuss, John Bantsolas made a motion to adjourn the meeting. Al Brunson seconded the motion. The meeting was adjourned at 12:02 p.m.	None	None

Submittal: The minutes of the above stated meeting are submitted for approval.

_____
Secretary of Meeting Date

Approval: Based on Committee consensus, the minutes of the above stated meeting are hereby approved as presented and/or corrected.

_____
Committee Chair Date

Partnership for Children of Cumberland County, Inc.

IT Policies and Procedures

Password Policy

Purpose

This policy establishes requirements for the creation, use, protection, and management of passwords used to access Partnership for Children of Cumberland County (PFC) systems, networks, and applications. The purpose of this policy is to safeguard organizational information assets, including systems that store or process Personally Identifiable Information (PII) and Protected Health Information (PHI), and to reduce the risk of unauthorized access.

Eligibility & Participation Requirements

This policy applies to all PFC employees, contractors, consultants, temporary staff, volunteers, and any other individuals who are granted access to PFC systems or data. All users are responsible for complying with the password standards and protection requirements outlined in this policy.

Password Standards

Network Passwords:

- Minimum length of 12 characters
- Combination of uppercase letters, lowercase letters, numbers, and special characters
- Not easily associated with the user
- Password reuse prohibited
- Multi-Factor Authentication (MFA) required

System-Level Passwords:

- Minimum length of 12 characters
- Combination of uppercase letters, lowercase letters, numbers, and special characters
- Not easily associated with the account owner
- Password reuse prohibited
- Must be changed every 90 days

Application Passwords:

- Minimum length of 12 characters
- Combination of uppercase letters, lowercase letters, numbers, and special characters
- Not easily associated with the account owner
- Password reuse prohibited
- Multi-Factor Authentication (MFA) required

Password Protection Requirements

- Passwords must not be shared

- Passwords must not be reused
- Passwords must not be transmitted electronically
- Passwords must not be written down or stored insecurely

Compromised Passwords

Employees must immediately change the password and notify IT at helpdesk@ccpfc.org

Non-Compliance

Failure to comply may result in disciplinary action

Partnership for Children of Cumberland County, Inc.

IT Policies and Procedures

Cybersecurity Training Policy

PURPOSE

Technical security controls are a vital part of our information security framework but are not sufficient by themselves to secure all information assets. Effective information security also requires awareness and proactive support of all staff, supplementing and making full use of technical security controls. This is obvious in the case of social engineering attacks and other current exploits being used, which specifically target vulnerable humans rather than IT and network systems

Lacking adequate information security awareness, staff are less likely to recognize or react appropriately to information security threats and incidents and are more likely to place information assets at risk of compromise. To protect information assets, all workers must be informed about relevant, current information security matters, and motivated to fulfill their information security obligations. This policy specifies the Cumberland County Partnership for Children internal information security awareness and training program to inform and assess all staff regarding their information security obligations

This policy applies throughout the organization as part of the corporate governance framework. It applies regardless of whether staff use computer systems and networks, since all staff are expected to protect all forms of information assets including computer data, written materials/paperwork, and intangible forms of knowledge and experience. This policy also applies to third party employees working for the organization whether they are explicitly bound (e.g. by contractual terms and conditions) or implicitly bound (e.g. by generally held standards of ethics and acceptable behavior) to comply with our information security policies

In general, this policy applies to all Cumberland County Partnership for Children employees and contractors with access to Cumberland County Partnership for Children systems, networks, company information, nonpublic personal information, personal identifiable information, and/or customer data

This policy will use the current version of training from KnowBe4 or recommended training.

Policy Requirements

All awareness training must fulfill the requirements for the security awareness program as listed below

- The information security awareness program should ensure that all staff achieve and maintain at least a basic level of understanding of information security matters, such as general obligations under various information security policies, standards, procedures, guidelines, laws, regulations, contractual terms, and generally held standards of ethics and acceptable behavior

- Additional training is appropriate for staff with specific obligations towards information security that are not satisfied by basic security awareness, for example Information Risk and Security Management, Security Administration, Site Security and IT/Network Operations personnel. Such training requirements must be identified in departmental/personal training plans and funded accordingly. The training requirements will reflect relevant prior experience, training and/or professional qualifications, as well as anticipated job requirements

- Security awareness and training activities should commence as soon as practicable after staff join the organization, generally through attending information security induction/orientation as part of the on-boarding process. The awareness activities should continue a continuous/rolling basis thereafter to maintain a reasonably consistent level of awareness

- Where necessary and practicable, security awareness and training materials and exercises should suit their intended audiences in terms of styles, formats, complexity, technical content, etc. Everyone needs to know why information security is so important, but the motivators may be different for workers focused on their own personal situations or managers with broader responsibilities to the organization and their staff

- The company will provide staff with information on the location of the security awareness training materials, along with security policies, standards, and guidance on a wide variety of information security matters

- **Cumberland County Partnership for Children Information Security Awareness Training**

  The Cumberland County Partnership for Children Information Technology department requires that each employee upon hire and at least annually thereafter successfully complete "**A New Hire's Guide to Security Awareness**".
  Certain staff may be required to complete additional training modules depending on their specific job requirements upon hire and at least annually. Staff will be given a reasonable amount of time to complete each course to not disrupt business operations

- **Simulated Social Engineering Exercises**

  The Cumberland County Partnership for Children Information Technology department will conduct periodically simulated social engineering exercises including but not limited to phishing (e-mail), vishing (voice), smishing (SMS), USB testing, and physical assessments. The Cumberland County Partnership for Children Information Technology department will conduct these tests at random throughout the year with no set schedule or frequency. The Cumberland County Partnership for Children Information Technology department may conduct targeted exercises against specific departments or individuals based on risk determination

- **Remedial Training Exercises**

  From time-to-time Cumberland County Partnership for Children staff may be required to complete remedial training courses or may be required to participate in remedial training exercises with members of the Cumberland County Partnership for Children Technology department as part of a risk-based assessment

Compliance & Non-Compliance with Policy

Compliance with this policy is mandatory for all staff, including contractors and executives. The Cumberland County Partnership for Children Information Technology department will monitor compliance and non-compliance with this policy and report to the executive team the results of training and social engineering exercises

- ## Non-Compliance Actions

  Certain actions or non-actions by Cumberland County Partnership for Children personnel may result in a non-compliance event (Failure)

  A Failure includes but is not limited to:

  - Failure to complete the required training within the time allotted
  - Failure of a social engineering exercise

  Failure of a social engineering exercise includes but is not limited to:

  - Clicking on a URL within a phishing test
  - Replying with any information to a phishing test
  - Opening an attachment that is part of a phishing test
  - Enabling macros that are within an attachment as part of a phishing test
  - Allowing exploit code to run as part of a phishing test
  - Entering any data within a landing page as part of a phishing test
  - Transmitting any information as part of a vishing test
  - Replying with any information to a smishing test
  - Plugging in a USB stick or removable drive as part of a social engineering exercise
  - Failing to follow company policies during a physical social engineering exercise

  Certain social engineering exercises can result in multiple Failures being counted in a single test. The maximum number of Failure events per social engineering exercise is three

  The Cumberland County Partnership for Children Information Technology department may also determine, on a case-by-case basis, that specific Failures are a false positive and should be removed from that staff member's total Failure count

- ## Compliance Actions

  Certain actions or non-actions by Cumberland County Partnership for Children personnel may result in a compliance event (**Pass**)

  A Pass includes but is not limited to:

  - Successfully identifying simulated social engineering exercises
  - Not having a Failure during a social engineering exercise (**non-action**)
  - Reporting real social engineering attacks on the Information Technology department

- ## Removing Failure Events Through Passes

Each Failure will result in a Remedial training or coaching event as described in Appendix A of this document. Subsequent Failures will result in escalation of training or coaching. De-escalation will occur when three consecutive Passes have taken place

Responsibilities and Accountabilities

Listed below is an overview of the responsibilities and accountabilities for managing and complying with this policy program

Cumberland County Partnership for Children Information Technology department: is accountable for running an effective information security awareness and training program that informs and motivates workers to help protect the organizations and the organization's customer information assets

System Administrator: is responsible for developing and maintaining a comprehensive suite of information security policies (including this one), standards, procedures and guidelines that are to be mandated and/or endorsed by management where applicable. Working in conjunction with other corporate functions, it is also responsible for conducting suitable awareness, training, and educational activities to raise awareness and aid understanding of staff's responsibilities identified in applicable policies, laws, regulations, contracts, etc.

All Managers: are responsible for ensuring that their staff and other workers within their responsibility participate in the information security awareness, training, and educational activities where appropriate and required
All Staff: are personally accountable for completing the security awareness training activities, and complying with applicable policies, laws, and regulations always

Appendix A – Schedule of Failure Penalties

The following table outlines the penalty of non-compliance with this policy. Steps not listed here may be taken by the Cumberland County Partnership for Children Information Technology team to reduce the risk that an individual may pose to the company

Failure Count	Resulting Level of Remediation Action
First Failure	**Mandatory completion of 2026 KnowBe4 Security Awareness Training - 30 minutes**
Second Failure	**Mandatory completion of 2026 KnowBe4 Security Awareness Training - 45 minutes & Basics of Phishing (with Quiz)**
Third Failure	**Mandatory completion of 2026 KnowBe4 Security Awareness Training - 45 minutes & Basics of Phishing (with Quiz) & How to Become A Human Firewall**
Fourth Failure	**Face to face meeting with their manager**
Fifth Failure	**Face to face meeting with their manager and Head of Human Resources**
Sixth Failure	**Face to face meeting with the CISO and the Head of Human Resources** - **Possibility that additional administrative and technical controls will be implemented to prevent further Failure events**
Seventh Failure	**Meeting with CIO, CEO and Head of Human Resources** - **Possibility that additional administrative and technical controls will be implemented to prevent further Failure events**
Eighth Failure	**Formal review of employment with Head of Human Resources**

	- **Possibility that additional administrative and technical controls will be implemented to prevent further Failure events**

Appendix B – Methods for Determining Staff Risk Ratings

The following is a list of situations that may increase the risk rating of a Cumberland County Partnership for Children staff member. Higher risk ratings may result in an increased sophistication of social engineering tests and an increase in frequency and/or type of training and testing

• Staff member email resides within a recent Email Exposure Check report
• Staff members are executive or VP (High value target)
• Staff member possesses access to significant company confidential information
• Staff members are using a Windows or Apple-based operating system
• Staff members use their mobile phone for conducting work-related business
• Staff member possesses access to significant company systems
• Staff personal information can be found publicly on the internet
• Staff member maintains a weak password
• Staff members have repeated company policy violations

Partnership for Children of Cumberland County, Inc.

IT Policies and Procedures

Data Retention Policy

Purpose

This policy establishes the guidelines for retaining and disposing of data collected, stored, or processed by the Partnership for Children of Cumberland County (PFC). The purpose is to ensure that all data is retained only for the period necessary to fulfill operational, legal, and regulatory requirements, and is properly destroyed when no longer needed. This policy applies to all PFC data stored on PFC-owned systems, devices, applications, or third-party platforms. It includes all data containing Personally Identifiable Information (PII) or Protected Health Information (PHI).

Policy Requirements

PFC retains only the data necessary to conduct business operations, fulfill reporting obligations, and comply with applicable laws and regulations. Reasons for data retention may include, but are not limited to:

- Ongoing services to individuals (e.g., newsletters, program participation updates, training).
- Compliance with federal, state, local, or funder-specific reporting requirements.
- Compliance with labor, human resources, and tax regulations.
- Operational or business needs.
- Security incident investigation.
- Litigation or records subject to a legal hold.
- Intellectual property or historical preservation needs.

Data Retention Guidelines

- Contributor data will be retained for the year of last contribution plus 7 years.
- Event participant data will be retained through the event and any follow-up distribution, plus 7 years.
- Subgrantee, subcontractor, and vendor data will be retained for the duration of the contract or agreement.
- Consultant (paid or pro bono) data will be retained through the consulting contract plus 7 years.
- Board member data will be retained for the duration of Board service plus 7 years.
- Tax-related data will be retained for 7 years.
- Operational system and application data will be retained for 7 years.
- Program proposals, reports, and management records will be retained for funder-required periods, but no more than 7 years unless required.

Data Destruction

When the retention period for a given category of data expires, PFC will destroy the data in accordance with the organization's Asset Management Policy. Employees who identify a potential business justification for retaining data beyond the stated retention period must notify their supervisor and provide written rationale. Exceptions require approval from PFC's Data Protection Officer, in consultation with legal counsel and approval from the president.

A litigation hold may be issued when legal counsel determines certain documents must not be destroyed. A litigation hold remains in effect until lifted by legal counsel.

Non-Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination, in accordance with PFC's disciplinary procedures.

Partnership for Children of Cumberland County, Inc.

IT Policies and Procedures

Backups Policy

Purpose

This policy establishes the requirements and responsibilities for the creation, storage, maintenance, and testing of electronic data backups for the Partnership for Children of Cumberland County (PFC). The purpose of this policy is to ensure that critical organizational data remains protected, recoverable, and accessible in the event of system failures, hardware malfunctions, cyber incidents, accidental deletion, natural disasters, or other unexpected disruptions.

Scope

This policy applies to all PFC data stored on PFC-owned systems, servers, workstations, cloud platforms, and third-party applications used for official business. It includes all data containing Personally Identifiable Information (PII) and Protected Health Information (PHI).

Backup Requirements

PFC requires the following backup schedule:

- Daily Backups: Critical operational data, financial data, HR data, child/family service data, and all databases.
- Weekly Backups: Full system backups for servers and cloud-managed systems.
- Monthly Backups: Archived system images stored for long-term redundancy.
- Annual Backups: A yearly system snapshot stored off-site for disaster recovery purposes.

Backup types may include:

- Full Backups: A complete copy of all selected data.
- Incremental Backups: Data changed since the last backup.
- Cloud-Synchronized Backups: Data automatically backed up via approved, secured cloud platforms.
- Encrypted Off-Site Backups: Long-term storage of mission-critical data in a secured secondary location.

Backup Storage Requirements

Primary and secondary storage locations are required to secure backup integrity and availability:

- Primary Storage: Backups will be stored on secure PFC-managed systems or approved cloud-based backup services.
- Secondary (Off-Site) Storage: A secure off-site or cloud-based location will be maintained to ensure continuity in the event of physical damage to PFC facilities.
- Encryption: All backup data must be encrypted to protect PII, PHI, and other sensitive information.

Backup Monitoring & Verification

PFC's IT personnel or contracted technology provider will monitor backup systems to ensure successful completion and detect any errors.

- Backup restoration tests will be performed at least quarterly.
- Any failed restore test must be addressed immediately.
- Documentation of all tests will be maintained by IT or the designated provider.

Data Recovery Procedures

- The employee or department must notify IT or the designated support provider immediately.
- IT will determine the most appropriate restore point based on the most recent successful backup.
- Recovery actions will follow established restoration procedures to ensure data integrity.
- Any recovery involving PII/PHI must follow privacy and security protocols.

Access & Authorization

- Only authorized personnel may configure, access, or restore backups.
- Backup logs, locations, and encryption keys must remain secured and may not be shared without proper authorization.

Retention of Backups

Backup retention must align with the Data Retention Policy. Backups containing expired data that has reached its retention limit must be securely destroyed in accordance with organizational data destruction standards.

Non-Compliance

Failure to comply with this policy may result in disciplinary action, up to and including termination, consistent with PFC's disciplinary procedures.

Family Resource Center
Space Availability Report

August 2023

Room #	Suite	Square feet	Notes:	
1163, 1164, 1165, 1166, common area @ 133.50 sf or 218.50 sf	130	657.5sf or 742.50sf	Available- Now	Option A with door / Option B without door and more common area
1149, 1150, 1151	135	441	Available- ?	
1129, 1131, 1132, 1133, 1134, 1135	165	867	Available- Now	
1117 - 1123	170	950	Available- ?	
2304,2305 combined		253	Available- 5/1/2026	
2306		106	Available- 5/1/2026	
2312, 2313	341	198	Taken by Gateway on 6/1/2026	
2330	326	374	Now Available	
2346		124	Available- 5/1/2026	
2408, 2413, 2414	411	1533	2406, 2407,2409, 2410 and 2412 are leased. Suite= sf 1686 -913 sf leased. 773 sf available.	2411 is a closet with 25 sq/ft
		5,503.50 SF		

RENT RATES	11/1/2023
Non Profit LM	$20.35
For Profit Over 300 SF	$21.45
For Profit Under 300 SF	$25.85
Deposit= 2 months rent	Renewals 10% or7%

	PFC	Others
Non Profit incl PFC :50.0%	39.0%	10.4%

For Profit: 39.1%

Leaseable Space of 27, 727 sf = Occupancy Rate: 88.6%

Un-Occupied: 11.4%