



Poughkeepsie Children's Cabinet Data Privacy Policy

1. Introduction

The Poughkeepsie Children's Cabinet (PCC) is committed to protecting the privacy and security of personal information of children, families, and individuals we serve. This policy outlines our practices for collecting, using, storing, and protecting personal data in compliance with applicable laws and regulations, including the Family Educational Rights and Privacy Act (FERPA), Children's Online Privacy Protection Act (COPPA), New York Education Law Section 2-d, and local requirements set by the Poughkeepsie City School District.

2. Types of Data Collected

PCC may collect the following types of personal information:

- Child and family demographic information
- Educational records
- Socioeconomic data
- Program participation data
- Assessment and evaluation data

3. Purpose of Data Collection

We collect and use personal data solely for the purpose of providing and improving our cradle-to-career services, including:

- Coordinating and delivering educational support programs
- Evaluating program effectiveness
- Identifying and addressing community needs
- Reporting aggregated, de-identified data to funders and partners



Poughkeepsie Children's Cabinet

4. Data Protection Measures

PCC implements the following measures to protect personal data:

- Encryption of data in transit and at rest
- Secure, access-controlled data storage systems
- Regular security audits and updates
- Employee training on data protection and privacy
- Strict access controls based on legitimate educational interest
- Implementation of a disaster recovery plan
- Regular data backups, including archiving of email
- Separation of duties in computer resource management

5. Data Sharing and Disclosure

PCC does not sell personal information under any circumstances. We may share data with:

- Authorized educational institutions and program partners;
- Researchers (using de-identified data only);
- Government agencies as required by law. All data sharing is subject to data protection agreements and only for purposes consistent with our mission.

Data Reporting and Small Group Privacy

To protect individual privacy in line with New York State Education Department policies and guidelines, PCC adheres to data suppression policy guidelines when reporting assessment results or other sensitive information. This includes, but is not limited to:

- Suppressing data where the number of students in a reported group is less than five (5).
- Using data ranges or other statistical methods to protect individual privacy when reporting on small groups.
- Implementing additional suppression techniques as necessary to prevent the identification of individuals in small groups or those with unique characteristics.



Poughkeepsie Children's Cabinet

6. Data Retention and Destruction

We retain personal data only as long as necessary to fulfill the purposes outlined in this policy or as required by law. When data is no longer needed, it is securely destroyed or de-identified in accordance with industry standards and best practices.

7. Individual Rights

Individuals have the right to:

- Access their personal data
- Request corrections to their data
- Opt-out of certain data collections
- File complaints about possible privacy breaches

8. Computer Resources and Network Use

8.1 Acceptable Use

- PCC computer resources are provided for educational and operational purposes only.
- Users must comply with all applicable laws and PCC policies when using computer resources.
- Each user is responsible for the proper use of their account and any activity conducted with it.

8.2 Prohibited Activities

The following activities are strictly prohibited:

- Using resources for commercial or personal gain
- Infringing on intellectual property rights
- Accessing or distributing inappropriate content
- Attempting to gain unauthorized access to systems or data
- Sharing account credentials
- Engaging in any form of cyberbullying or harassment



Poughkeepsie Children's Cabinet

- Installing unauthorized software

8.3 No Expectation of Privacy

Users should have no expectation of privacy when using PCC computer resources. PCC reserves the right to monitor and access any data stored on or transmitted through its systems.

9. Data Breach Notification

In the event of a data breach, PCC will:

- Promptly notify affected individuals and appropriate authorities as required by law
- Cooperate with law enforcement and regulatory bodies in any investigation
- Take immediate steps to contain and mitigate the breach
- Review and update security protocols to prevent future incidents