DC
PUBLIC
CHARTER
SCHOOL
BOARD

POLICY TITLE:	
Data Access Security Policy	
ADOPTION/EFFECTIVE DATE:	MOST RECENTLY UPDATED:
September 16, 2013	N/A

PURPOSE

PCSB collects student-level data directly from charter LEAs and campuses for local and federal reporting; accountability, including Performance Management Framework calculations; monitoring of legal compliance; internal analysis; and other purposes as necessary. To support data quality assurance efforts and analysis, PCSB makes available student-level and aggregated data to the schools and their authorized staff. In order to comply with FERPA, PCSB and schools must ensure that only school-determined authorized staff have access to student-level data, including enrollment, demographic, attendance, discipline, and academic data.

POLICY

Beginning in School Year 2013-14, all public charter Local Education Agencies ("LEAs") and their constituent campuses will be responsible for ensuring that only authorized school staff have access to the school's student-level data in PCSB's data systems, including but not limited to ProActive, SharePoint, Epicenter, and Secure File Transfer Protocol ("SFTP") sites. Accordingly, each LEA will be responsible for the following:

- Reviewing, before the beginning of each school year, staff access to all applicable data systems and notify PCSB of any individuals who should not have access to the systems. PCSB will help schools in this process through training, documentation, and, as necessary, hands on assistance.
- Requesting additional staff access to PCSB's data systems on an as-needed basis.
- Notifying PCSB in writing of any contractors, consultants, or other third parties who it has authorized to access the school's student-level data and communicate with PCSB on its behalf.
- Providing PCSB with the contract that delineates the measures in place to ensure compliance with the Family Educational Rights Privacy Act ("FERPA").
- Notifying PCSB within 5 business days after staff or consultants with access to PCSB's data systems leave their position or have their contracts terminated. PCSB will deactivate those individuals' access to ProActive, SharePoint, Epicenter, and any other data systems in place within 5 business days of receiving the notice.
- Prohibiting school staff from sharing logins to ProActive or Epicenter. If additional staff members need access to these databases, the school will request access for each individual.

Board Approval Acknowledged By:

____

Darren Woodruff
DC PCSB Board Chair

Disclaimer: This publication is designed to provide information on the subject matter covered. It is distributed with the understanding that the publisher is not engaged in rendering legal, accounting or other professional services. Readers will be responsible for obtaining independent advice before acting on any information contained in or in connection with this policy.