a) Personenbezogene Daten sind „Daten, die sich einer Person eindeutig zuordnen lassen“.
Es gelten die Prinzipien
   i. Verbot mit Erlaubnisvorbehalt:
   Datenverarbeitung nur durch spezielle Gesetze oder mit Einwilligung erlaubt
   ii. Datenminimierung: nur nötige Daten werden verarbeitet, und so bald wie möglich gelöscht
   iii. Zweckbindung: erhobene Daten dürfen nur zum angegebenen Zweck verarbeitet werden
   iv. Transparenz: Personen, deren Daten verarbeitet werden, sollen darüber Bescheid wissen
   v. Erforderlichkeit: nur Daten, die für einen Zweck erforderlich sind, dürfen verarbeitet werden

b) Lehrer: unterrichtete Fächer

Schüler:
Vor- und Nachname, Klasse, Erziehungsberechtigte
Fehlzeiten, deren Grund und ob diese entschuldigt sind
Bemerkungen, z.B. über Fehlverhalten

Erziehungsberechtigte:
Vor- und Nachname, Namen der Kinder
Rückschlüsse / Vermutungen zur Qualität ihrer Erziehung, z.B. durch Anzahl unentschuldigter Fehlstunden oder Bemerkung über ihre Kinder

c) Bedenkenlos darf gespeichert werden, was öffentlich zugänglich ist:
Namen der Lehrer und Kürzel, Unterrichtsfächer der Lehrer
Informationen über Fächer (Bezeichnung, Wochenstunden, Klassen)

d) Mögliche Antworten:
Erforderlichkeit ist bei den erhobenen personenbezogenen Daten wohl gegeben, da sie im Schulalltag benötigt werden.
Die Erlaubnis zur Erhebung der Daten und Transparenz dürfte durch die Schulpflicht und das Schulgesetz geregelt sein.
Die Zweckbindung von Daten über Schüler dürfte vorsehen, dass Lehrer über Leistungen und Verhalten der Schüler informiert sind. Eltern über das Verhalten von Kindern zu informieren, die nicht ihre eigenen sind, ist nicht Zweck der Datenerhebung und damit nicht zulässig, daher ist die Einsicht in die Bemerkungen problematisch.
Probleme können auch bei der Datenminimierung entstehen. Personenbezogene Daten müssen gelöscht werden, sobald sie nicht mehr benötigt werden.

e) Das Hauptrisiko ist der Zugriff durch Unbefugte, die unerlaubt Zugriff auf die Datenbank erhalten und dann z.B. Daten veröffentlichen und damit Personen schädigen.

Sicherer wird eine Datenbank durch Erschweren solcher illegalen Zugriffe:
Die Computer des Sekretariats dürfen nicht jedermann zugänglich sein und sollten durch ein sicheres Passwort geschützt sein. Falls der Zugriff über das Internet auf die Datenbank möglich ist, ist eine verschlüsselte Verbindung und ein sicheres Passwort notwendig.

Software kann auch Programmierfehler enthalten, die Sicherheitslücken öffnet.
Daher sollte die Software ausreichend getestet sein.