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)
   i. Lehrer: unterrichtete Fächer
   ii. Schüler:
   Vor- und Nachname, Klasse, Erziehungsberechtigte
   Fehlzeiten, deren Grund und ob diese entschuldigt sind
   Bemerkungen, z.B. über Fehlverhalten
   iii. 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

d)
   i. Die Erforderlichkeit ist bei den erhobenen personenbezogenen Daten gegeben, da sie im Schulalltag benötigt werden.
   ii. Die Erlaubnis zur Erhebung der Daten sowie die Transparenz der Erhebung gegenüber den Beteiligten ist durch die Schulpflicht und das Schulgesetz geregelt.
   iii. Die Zweckbindung der Daten sieht vermutlich vor, dass Lehrer*innen über Leistungen und Verhalten der Schüler*innen 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 sollten Eltern keine Einsicht in die Bemerkungen von Klassebucheinträgen haben, die in diesem System Informationen über beliebige Schüler*innen enthalten können.
   iv. Bei der Datenminimierung können Probleme entstehen. Personenbezogene Daten müssen gelöscht werden, sobald sie nicht mehr benötigt werden.

e)
   i. Ein Risiko ist der Zugriff durch Unbefugte (z.B. Hacker) auf die Datenbank, die dann z.B. Daten veröffentlichen und so Personen schädigen können.
   Sicherer wird die 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 notwendig, außerdem Sicherheitsvorkehrungen für das Netzwerk des Servers wie z.B. eine Firewall. Das System sollte regelmäßig Updates erhalten, damit eventuelle Sicherheitslücken geschlossen werden.
   ii. Ein weiteres Risiko betrifft die Verfügbarkeit der Daten. Der Datenbankserver könnte z.B. durch ein technisches Problem ausfallen oder durch einen Brand zerstört werden.
   Für solche Fälle braucht es regelmäßige Backups, die Verteilung auf mehrere Server etc.