Schule am Drachenfeld
Schule mit Förderschwerpunkt geistige Entwicklung
und einer Abteilung körperliche und motorische Entwicklung

Anne-Frank-Straße 5
64711 Erbach

Telefon 0 60 62 · 8 09 62 0
Telefax 0 60 62 · 8 09 62 10

E-Mail info@drachenfeld.de
Web www.drachenfeld.de

Datenschutzvereinbarung

Allgemeines

Im Umgang mit personenbezogenen Daten ist besondere Sorgfalt anzuwenden. Aus diesem Grund wurden folgende Vereinbarungen zur täglichen Arbeit mit datenschutzrelevanten Daten als Handreichung formuliert und durch das Kollegium mit Konferenzbeschluss vom 14.02.2019 verabschiedet.

E-Mail und Cloud

Jede Lehrkraft erhält einen individuellen E-Mail-Account mit persönlichem Passwort. Ebenso verhält es sich mit dem Zugang zur schulinternen Cloud. Jede Lehrkraft trägt die Verantwortung für das eigene Passwort selbst. Es darf nicht weitergegeben werden. Die Kommunikation über die @drachenfeld.de-Accounts und die Cloud ist mit einer 128-bit User-to-User-SSL-Verschlüsselung geschützt. Eine zusätzliches Verschlüsselungsplugin (PGP; S/MIME) erhöht den Sicherheitsstandard. Schulrelevante E-Mails sollen ausschließlich mit @drachenfeld-Accounts verschickt werden, um die Daten zu verschlüsseln und zu sichern. Bei Abrufen der E-Mails über einen öffentlichen Webzugang oder einen Lehrerarbeitsplatz ist sicherzustellen, dass der E-Mail-Client erfolgreich beendet und abgemeldet ist und kein Passwort lokal in dem öffentlichen Computer gespeichert wird. Das Löschen des Browserverlaufs kann die Sicherheit erhöhen. Der Serverstandort ist Erbach bzw. Berlin (entgegen Google und Dropbox).

Drachenfeld-WLAN

Jede Lehrkraft erhält einen vorkonfigurierten, verschlüsselten Stick mit Anleitung zur Sicherung personenbezogener sensibler Daten. Die Synchronisationsordner der Cloud sowie der persönliche Ordner werden permanent gespiegelt, um Datenverlusten vorzubeugen. Für Daten außerhalb dieser Ordner tragen die Lehrkräfte selbst Sorge zum Backup. Durch die Verschlüsselung ist die Datensicherheit auf den Sticks bei Verlust gewährleistet.

Geschützter Bereich/www.drachenfeld.de

Der Zugriff auf den geschützten Bereich auf www.drachenfeld.de erfolgt über ein gemeinsames Passwort. Dieses Passwort darf nicht weitergegeben werden. Das Passwort wird regelmäßig geändert. Das Abmelden (Log-out) trägt dazu bei, dass der geschützte Bereich sicher bleibt und ist unbedingt durchzuführen.
Der Zugriff auf das schuleigene WLAN ist mit einem allgemeinen WPA2-Kennwort gesichert, welches bei Fabian Moos erfragt werden kann. Dieses Passwort darf nicht weitergegeben werden. Insbesondere nicht an Assistentinnen und Assistenten, da über das WLAN Zugriff auf das Computernetzwerk möglich ist. Die Verwaltungsrechner sind in einem separaten Netzwerk abgesichert.
Die Arbeit am eigenen Computer ist tägliche Praxis. Da der Computer in der Regel auch für private Zwecke genutzt wird (oder mobil ist), sind einige Grundsätze einzuhalten:

- Der Computer ist mit einem Passwort vor fremden Zugriffen zu schützen (z.B. bei Inaktivität von 15 Minuten).
- Eine Zwei-Faktor-Authentisierung bietet zusätzlichen Schutz
- Dokumente mit schülerbezogenen Daten und Adressen sollen ausschließlich auf dem zur Verfügung gestellten verschlüsselten Stick gespeichert und verarbeitet werden.
- Backups und Datensicherungen sollten nur verschlüsselt erfolgen.
- Der eigene Computer ist so zu schützen, dass kein Zugriff auf die personenbezogenen Daten über WLAN, Bluetooth oder andere Schnittstellen möglich ist (Sicherheitseinstellungen: Fremdzugriff neuer Geräte verifizieren).
- Der eigene Computer sollte regelmäßig auf Viren, Trojaner oder Schadsoftware überprüft werden. Auch inaktive Schadsoftware kann sich z.B. durch Weiterleiten von infizierten E-Mails von einem System auf das andere übertragen. Sollte man unerwünschte Aktivitäten auf dem eigenen Rechner feststellen (z.B. durch Viren o.ä.), ist die Verbindung zur Cloud zu trennen und ein E-Mail-Austausch bis zur Bereinigung zu unterlassen. Unregelmäßigkeiten im E-Mailverkehr oder in der Cloud-Datensynchronisation sollten unverzüglich fabian.moos@drachenfeld.de und sven.orth@drachenfeld.de gemeldet werden.

- Zeugnisse, Stellungnahmen etc., welche immer schülerbezogene Daten enthalten, sollten nach Möglichkeit nicht zu Hause ausgedruckt werden. Fehl- oder Korrekturausdrucke sind vor dem Entsorgen in der Papiertonne zu schreddern. Die Endform der Zeugnisse wird über die Laserdrucker in der Verwaltung realisiert (Erstseite Farblaserdruck, Folgeseiten Monochromlaserdruck.)
- Bei Datenpannen (Verlust des Sticks, Kapern des Computers etc.) ist SOFORT die Schulleitung und der Datenschutzbeauftragte zu informieren.

Mobiltelefon

Für die Nutzung des Mobiltelefons gelten ähnliche Grundvoraussetzungen. Ergänzend hierzu soll noch auf die Sozialen Netzwerke hingewiesen werden.

- Von einer privaten Kontaktpflege der Lehrkräfte (und Assistierenden) mit Schülerinnen und Schülern (und ggf. Eltern) der SAD in sozialen Netzwerken ist ausdrücklich abzuraten. Dies betrifft insbesondere sogenannte Freundschaften.
- Personenbezogene Daten, Dokumente und Krankmeldungen dürfen über soziale Netzwerke nicht kommuniziert werden.
- Wir empfehlen die Einrichtung einer Fernlöschung

BFZ-Arbeit

Die Lehrkräfte in der BFZ-Beratungsarbeit erhalten zusätzlich einen eigenen, individualisierten BFZ-Cloud-Zugang. Um Datenverlusten vorzubeugen und einen schnellen Zugriff auf aktuelle Daten zu gewährleisten, verpflichten sich die BFZ-Kolleginnen – und Kollegen zur regelmäßigen Sicherung Ihrer Dokumente in der BFZ-Cloud. Dies wird dadurch vereinfacht, dass ein gespiegelter Dokumentordner lokal auf dem zur Verfügung gestellten, verschlüsselten Stick unter xy_crypt vorliegt. So kann man auch »offline« arbeiten, die geänderten Dokumente aktualisieren sich mit der Cloud bei der nächsten Anmeldung automatisch. BFZ-Lehrkräfte müssen bei Verwendung ihres eigenen Computers besondere Sorgfalt bei der Verschlüsselung des Computers und der Daten walten lassen (siehe Punkt: Arbeit am eigenen Computer). Gutachten und Stellungnahmen sind über die Farbdrucker in der Verwaltung auszudrucken, Fehldrucke sind vor der Entsorgung in der Papiertonne zu schreddern.

Akten, Förderpläne, Zeugnisse

Die pädagogischen und medizinischen Schülerinnen-und Schülerakten sowie die Zeugnisse und Förderpläne enthalten sensible persönliche Daten die besonders schützenswert sind. Aus diesem Grund werden diese Dokumente in verschlossenen Schränken und Räumen vor unbefugtem Zugriff geschützt. Grundsätzlich haben nur jene Personen Zugriff auf diese sensiblen Daten, die mit diesen Daten arbeiten müssen. Assistierenden, Praktikantinnen und Praktikanten ist der Zugang zu diesen Akten nur in Begleitung zu gewähren. Die Akten dürfen nicht kopiert oder gescannt (fotografiert) werden und das Schulgebäude nicht verlassen.
Datenblätter und Förderpläne, welche als Kopie in den Klassen vorliegen, müssen in einem Schrank verschlossen sein.

Digitaler Datenaustausch

Sollen an andere Institutionen Dokumente (Stellungnahmen, Protokolle etc.) digital weitergegeben werden, so darf dies nur als (verschlüsseltes) PDF-Dokument erfolgen. Dies gilt auch für interne Protokolle von Konferenzen, Arbeitsgruppen, Förderpläne, Zeugnisse, die digital gespeichert werden sollen. Eine Verschlüsselung des versendeten PDFs bietet zusätzliche Datensicherheit. PDF-Dateien sind offenen Office-Dateien vorzuziehen, da letztere (ggf. ohne Nachweis) veränderbar sind und somit nicht fälschungssicher sind. Ein Passwortschutz in Officedokumenten ist nicht sicher.

Datenblätter, Bildfreigaben

Die Klassenteams sorgen dafür, dass es für jede Schülerin und jeden Schüler aktuelle Datenblätter und Einverständniserklärungen gibt. Diese sind im Original vorne in der Schülerakte abzuheften. Sie enthalten eine Entscheidung zur Bildfreigabe. Die Bildfreigabe ist ausdrücklich auf die Nutzung von Bildaufnahmen für die

Homepage der Schule und Pressemitteilungen über die Schule beschränkt. Es sollen niemals Schülerinnen- und Schülerbilder mit Namen veröffentlicht werden.
Abbildungen von Schülerinnen und Schülern dürfen nicht ohne vorherige Erlaubnis der Eltern an Dritte weitergegeben werden, dies betrifft auch Kooperationsprojekte. Für diese Fälle sind eigens Bildfreigaben einzuholen, die die Nutzung der Bilder genau beschreiben. In sozialen Netzwerken (Facebook, WhatsApp, Twitter o.ä.) sollten generell keine Bilder der Schülerinnen und Schüler gepostet werden.

Nutzungsprofile und Alternativen

Gerade in der Nutzung von Facebook, WhatsApp, Google, Microsoft etc. sollte jeder/jedem bewusst sein, dass Nutzungsprofile angelegt werden. Aus diesem Grund ist es empfehlenswert

- die Cookies, den Cache und das Verlaufsprotokoll jedes Browsers regelmäßig zu löschen
- ein Verschlüsselungsplugin (PGP;s/mime) generell für E-Mails zu nutzen
- für Online-Banking einen getrennten Browser zu nutzen
- Passwortmanager zur Erstellung und Verwaltung sicherer Passwörter (über 20 Zeichen) zu verwenden
- ggf. alternative Suchmaschinen zu nutzen (z.B. Quant.com)
- ggf. alternative Messengerdienste zu nutzen (z.B. Signal)
- Facebook nach Besuch „richtig“ schließen
- ggf. die Einwilligung in sog. „Produktverbesserungen“ zu vermeiden (Haken herausnehmen)

Die meisten dieser Schritte dienen auch der eigenen Datensicherheit.