IT-Richtlinien an den Schulen des DSSV

Diese IT Politik gilt für Mitarbeiter und Schüler sowie deren Eltern an den Schulen des DSSV.

Ziel der IT Politik ist es, die persönlichen Daten der Schüler und Mitarbeiter zu beschützen. Außerdem soll mit der IT Politik gewährleistet werden, dass alle Mitarbeiter dazu im Stande sind, die Schüler darüber zu informieren, welche Anforderungen zur IT Sicherheit von ihnen eingehalten werden müssen.

Die IT Politik wird einmal jährlich in Zusammenarbeit zwischen dem Schulamt und dem IT-Center revidiert.

Password

Alle Schülerinnen und Schüler bekommen zum Schulanfang ein Uni-login, mit dem sie sich in die PCs der Schule sowie in Office365 einloggen können. Das Password wird von STIL zugeteilt, kann aber in „mitunilogin“ geändert werden. Die Schule kann das Password des Schülers einsehen und es zurücksetzen.[1]

Die Lehrer erhalten ebenfalls bei ihrer Einstellung ein Unilogin, mit dem sie sich in die PCs der Schule sowie in Office365 einloggen können. Das Password der Lehrer ist nicht einsehbar, kann aber ebenfalls in „mitunilogin“ geändert werden.

Es gibt zum jetzigen Zeitpunkt von Unilogin noch keine Regeln oder Möglichkeiten, dass der Nutzer sein Password nach einem bestimmten Zeitpunkt ändern muss. Deshalb ist es wichtig, dass der Nutzername und das Password nicht sichtbar herumliegen.

Lehrer und Schüler loggen sich in ein pädagogisches Netzwerk ein, das vom administrativen Netzwerk getrennt ist.

Das administrative Personal logt sich mit besonderen Codes in das administrative Netzwerk. Das Password kann mit Hilfe von CTRL-ALT-DEL geändert werden. Eine neue Password Politik für das administrative Personal wird am 1. August 2019 in Kraft treten. Hier gilt, dass der Nutzer gebeten wird alle drei Monate das Password zu ändern.[2]

Für alle gilt, dass das der Nutzername und das Password persönlich sind und nicht an andere ausgehändigt werden darf.

1 Im Laufe von 2019 werden von Unilogin Änderungen kommen.
2 Bisher gilt diese Regelung nicht für Schüler und Lehrer. Wir warten eine Rückmeldung von STIL ab.

Zugriff zu Programmen, Unterrichtsportalen, u.ä.

Um zu gewährleisten, dass Lizensabsprachen und die GDPR[3] eingehalten werden, sind die Schulen des DSSV aufgefordert, beim Kauf von Programmen oder Zugriff zu Unterrichtsportalen sich vom IT-Center beraten zu lassen.

Wenn Probeversionen heruntergeladen werden, muss gewährleistet sein, dass eine „databe-handleraftale" mit der jeweiligen Firma eingegangen worden ist. Dies muss durch die Schulleitung und das IT-Center gehen.

Der DSSV benutzt ausschließlich echte und lizensierte Programme.

Die Schule hat in Bezug auf Personendaten die Verantwortung für alle Daten. Deshalb ist es nicht erlaubt persönliche Daten auf private Computer zu überführen/kopieren, d.h. auf private USB Sticks, private E-Mails oder private PCs.

Backup und Sicherheitskopien
Das IT-Center ist dafür verantwortlich, dass von allen Daten in allen Netzwerkservern (päd. und adm. Netzwerk) Sicherheitskopien erstellt werden.

Die E-Mails liegen bei Microsoft in einer Offeice365 Exchange Sicherheitslösung.

Die Schüler haben die Möglichkeit ihre Dokumente in Onedrive via office.com zu speichern.

Die Lehrer haben Zugriff zu persönlichen und gemeinsamen Netzwerklaufwerken im pädagogischen Netzwerk und zu Onedrive in office.com.

Die administrativen Mitarbeiter haben Zugriff zu persönlichen und gemeinsamen Netzwerkserver im administrativen Netz und zu Onedrive in office.com.

Die Schulen, die Zugriff zu Skoleintra haben, haben zudem die Möglichkeit ihre Daten in Skoleintra zu speichern.

Der einzelne Mitarbeiter ist selber für ein Backup verantwortlich, wenn seine Daten nicht auf dem Netzwerkserver gespeichert sind. Persönliche Daten dürfen nicht auf lokalen PCs gespeichert werden, sondern ausschließlich auf dem Netzwerkserver und auf Skoleintra.

Sicherheit

3 General Date Protection Regulation (Persondataforordning)

Alle Mitarbeiter tragen Verantwortung für die Sicherheit an den Schulen und tragen dazu bei die Schüler darüber zu informieren, wie man am besten im Internet verkehrt und dabei seine persönlichen Daten schützt. Folgende Regeln müssen deshalb eingehalten werden:

- Die Computer werden ausgeschaltet wenn der Mitarbeiter nach Hause geht.
- Wenn mehrere Schüler an einem PC arbeiten, muss sich jeder nach der Benutzung ausloggen.
- Der Computer muss nach Benutzung mit einer Bildschirmsperre gesichert werden (Windowstaste + L).
- Alle Handys müssen mit einer Bildschirmsperre versehen sein, wenn sie mit Mails und/oder Kalendern synchronisiert sind, da diese Daten sonst frei zugängig sind, wenn das Handy offen herumliegt.
- Es ist nicht erlaubt Material einzusehen oder von schulischen Geräten oder Netzwerk der Schule zu verschicken, dessen Inhalt pornografisch, politisch/religiös extremistisch oder diskriminierend ist.
- Inhalte von Mails müssen gegenseitigen Respekt und Höflichkeit widerspiegeln
- Mails mit persönlichen Daten müssen als „sikker mail“ verschickt werden.

Internet und E-Mails

Das Internet ist ein wichtiger Bestandteil des Unterrichtes wenn es um die Suche von Informationen geht. Deshalb gelten folgende Regeln:

- Schüler dürfen Programme nur in Absprache mit dem Lehrer downloaden.
- Es ist nicht erlaubt Material von pornografischen Homepages oder Homepages weiterzuleiten, die einen politischen/religiösen extremistisch oder diskriminierenden Charakter haben.
- Um zu gewährleisten, dass die Schule die GDPR einhält, müssen alle Mitarbeiter ihre Arbeitsmail benutzen, die ihnen von der Schule zur Verfügung gestellt wird. Private E-Mail Adressen dürfen nicht in dienstlichen Zusammenhängen benutzt werden.

Soziale Medien

Facebook kann ein gutes Medium sein um auf seine Schule aufmerksam zu machen, aber in Verbindung mit der Nutzung von Facebook gibt es einige Dinge, die beachtet werden müssen.

- Eine Facebook Seite, die die Schule nach Außen repräsentiert, sollte von der Schule / von der Schulleitung errichtet werden und nicht von Eltern.
- Wenn Gruppen für einzelne Klassen errichtet werden, sollten es geschlossene Gruppen sein.
- Es dürfen auf der Facebook Seite keine Daten eingesammelt werden.
- WhatsApp und Messenger dürfen intern unter Mitarbeitern benutzt werden, aber nicht in dienstlichen Zusammenhängen zwischen Mitarbeitern und Eltern.
- Chat kann über die Funktion in Office 365 stattfinden.

Virus und Spam

Auf allen PCs im administrativen Netzwerk sind Antivirusprogramme installiert, von denen automatisch Updates gemacht werden. Alle Schüler-PCs und Lehrer-PCs sind mit einem Antivirusprogramm versehen. Es ist nicht erlaubt andere Antivirusprogramme zu installieren.

Es ist erlaubt eigene private PCs im Netzwerk der Schule zu benutzen, sie müssen aber mit einem Antivirusprogramm versehen sein. Das IT-Center empfiehlt AVIRA.

Um das Risiko eines Virus oder Hackerangriffs auf den PCs der Schule zu minimieren, ist es wichtig, dass die Mitarbeiter folgende Regeln einhalten:

- Öffne nie E-Mails von unbekannten Absendern, die nicht reell aussehen.
- Öffne nie Anhänge von unbekannten Absendern.
- Sei vorsichtig beim Anklicken von Links in Mails von zweifelhaften Absendern.
- Checke regelmäßig die Spam Mailbox.
- Blockiere Absender von Spam Mails.

Handys
Es ist erlaubt seine Arbeitsmails auf dem privaten Handy zu laden, aber das setzt voraus, dass das Handy mit einer Bildschirmsperre versehen ist, wenn es nicht benutzt wird. Sollte das Handy verloren gehen, muss die IT-Abteilung kontaktiert werden, um die Mailfunktion zu schließen.

Da die Schule die Verantwortung für alle Daten trägt, ist es nicht erlaubt private Handys oder Tablets für die Aufnahme von Fotos/Videos von Eltern/Schülern zu benutzen. Hierfür sollten Geräte der Schule benutzt werden. Hierbei muss auf darauf geachtet werden, ob eine Einverständniserklärung der Eltern vorliegt.

BYOD – Bring your own device
In den Schulen ist es erlaubt eigene private IPads, Tablets o.ä. als Arbeitsgerät zu benutzen, aber es setzt folgendes voraus:

- Die automatische Bildschirmsperre muss aktiviert sein
- Die IT-Abteilung leistet nur in Verbindung mit dem Zugang zu Office 365, Skoleintra und anderen schulischen Programmen Support. Nicht für Hardware

Daten und E-Mail in Verbindung mit der Beendigung der Anstellung

Der Zugriff zum Netzwerk der Schule, der Arbeitsmail und zu Daten wird bei Beendigung der Anstellung deaktiviert. Daten und E-Mails werden 2 Monate nach Beendigung der Anstellung gelöscht, es sei denn die IT-Abteilung wird in besonderen Fällen gebeten damit zu warten. Dies gilt auch für Mitarbeiter im administrativen Bereich.

Daten und E-Mails in Verbindung mit der Abmeldung eines Schülers
Der Zugriff zum Netzwerk der Schule wird bei der Abmeldung eines Schülers deaktiviert. Nach zwei Monaten wird der Schüler aus dem Netzwerk der Schule gelöscht.

Apenrade
16.05.2019