IT-Politik an den Schulen des DSSV

Diese IT Politik gilt für 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 und ein Login für SchulPC's und Office365. Unilogin wird für Online Portale wie z.B. Gyldendal, Test og prøver, netprøver.dk benutzt.
Das Passwort für Unilogin wird bei dem ersten Login angezeigt. Es wird von STIL(Styrelsen for IT & Læring)aus gesteuert. Das Passwort kann von Lehrern und Eltern zurückgesetzt werden. Die Eltern benutzten dafür mitunilogin.dk. Infos darüber ist bei jeder Schule erhältlich.
Das andere Login wird von dem IT-center zugeteilt. Das Passwort hierfür kann auf diese Seite geändert werden – www.ssp.ds-n.dk. Hat man einen Verdacht das Passwort abgelauscht worden ist, soll man es umgehend ändern.

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

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

Schule als Datenverantwortlicher

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

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

Sicherheit

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:

- 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).
- 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 Unterrichts 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.

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

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

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-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.