Schulgemeinde Steinegg

Reglement über die Informatiknutzung

vom 24. Juni 2013

I. Allgemeine Bestimmungen

Art. 1

Geltungsbereich

[1]Dieser Beschluss regelt die Informatiknutzung der Mitarbeiter* im Rahmen ihrer Anstellung und der Schüler im Rahmen des Unterrichts.

[2]Werden Informatikmittel, die nicht der Schulgemeinde gehören, oder fremde Internetzugänge und E-Mail-Dienste genutzt oder nutzen andere Personen als Mitarbeiter und Schüler Informatikmittel der Schulgemeinde, gilt der Beschluss sinngemäss.

[3]Für Schulbehördenmitglieder regelt der Schulrat das Erforderliche mittels interner Weisung.

Art. 2

Informatik Sicherheitsbeauftragter

Die Schulbehörde bestimmt einen Informatik-Sicherheitsbeauftragten und einen Stellvertreter. Im Einvernehmen mit dem Kanton können der kantonale Informatik-Sicherheitsbeauftragte und sein Vertreter diese Funktion übernehmen.

II. Nutzung von Informatikmitteln

Art. 3

Informatikmittel

[1]Informatikmittel sind Geräte und Teile davon, die in der Bearbeitung, Speicherung oder Übermittlung von elektronischen Daten eingesetzt werden können.

Als Informatikmittel gelten insbesondere:

1. Computer aller Art, einschliesslich Notebooks, digitale Assistenten und Smartphones;
2. Datenträger aller Art, beispielsweise Harddisks, Disketten oder USB-Sticks;
3. EducaNet, AINet, Internet und E-Maildienste;
4. Elektronische Daten und Programme.

* Die Verwendung der männlichen Bezeichnung gilt sinngemäss für beide Geschlechter.

Art. 4

Nutzungszweck

[1]Die Nutzung von Informatikmitteln dient geschäftlichen oder schulischen Zwecken.

[2]Die private Nutzung durch den Mitarbeiter ist punktuell erlaubt. Sie darf weder die Leistung des Mitarbeiters noch die Informatikstruktur beeinträchtigen noch Zusatzaufwand bringen oder Sicherheitsrisiken bergen. Sie kann in begründeten Fällen eingegrenzt oder verboten werden.

[3]Die gesamte Nutzung von Informatikmitteln durch Schüler untersteht der Anordnung der Lehrkräfte.

Art. 5

Datenspeicherung

[1]Die Datenspeicherung auf Geräten, die am EducaNet angeschlossen sind, ist auf einem EducaNet- oder AINet-Serverlaufwerk vorzunehmen.

[2]Private Daten sind in der Regel auf privaten Datenträgern, zum Beispiel auf einem dafür vorgesehenen USB-Stick, zu speichern.

[3]Die Speicherung von geschäftlichen oder schulischen Daten auf entfernten Systemen, beispielsweise in Clouds, ist nicht erlaubt.

Art. 6

Fremdprogramme und Fremdgeräte

[1]Programme oder Geräte gelten als fremd, wenn sie nicht zur Verfügung gestellt wurden oder vom Schulrat, in Absprache mit dem Amt für Informatik (AFI), nicht ausdrücklich zugelassen sind.

[2]Es dürfen keine Fremdprogramme installiert oder Fremdgeräte angeschlossen werden, es sei denn, der geschäftliche oder schulische Auftrag verlangt diese Verwendung.

[3]Vertrauliche Geschäftsdaten sind auf Fremdgeräten verschlüsselt abzulegen und dort zu löschen, wenn sie nicht mehr gebraucht werden.

Art. 7

Sicherheit

[1]Die Mitarbeiter und Schüler schützen die von ihnen verwendeten Informatikmittel gemäss dem Stand der Technik vor unberechtigtem Gebrauch, insbesondere durch

1. Sperren der Computer oder Abmelden vom System beim Verlassen des Arbeitsplatzes;
2. Geheimhaltung der persönlichen Passwörter;
3. Sorgfältige Aufbewahrung und Überwachung mobiler Geräte.

[2]Virenverdächtige Programme, Dateien, E-Mails und Anhänge dürfen nicht geöffnet oder weitergeleitet werden und sind zu löschen. In Zweifelsfällen kann Rücksprache mit dem AFI genommen werden.

[3]Die Mitarbeiter informieren den Vorgesetzten bei sicherheitsrelevanten Risiken umgehend, beispielsweise bei einem Verlust eines mobilen Geräts. Schüler informieren die verantwortliche Lehrkraft.

Art. 8

Anschluss an Netzwerke

Informatikmittel dürfen nicht gleichzeitig im EducaNet oder im AINet und in einem anderen Netzwerk, beispielsweise in einem öffentlichen, drahtlosen Netz, angeschlossen sein.

Art. 9

Veränderungen und Kopien

[1]Veränderungen an den bereitgestellten Informatikmitteln, insbesondere an der Konfiguration von Hardware, an den Systemeinstellungen und an der Software, und die Umgehung oder Entfernung von Sicherheitsvorkehrungen sind nicht erlaubt.

[2]Das Kopieren von Programmen ist, unter Vorbehalt von Sicherungskopien oder der ausdrücklichen Einwilligung des AFI, unzulässig.

Art. 10

Pflichten beim Austritt

[1]Bei einem Austritt aus dem Dienstverhältnis sind die zur Verfügung gestellten Informatikmittel aufgeräumt zurückzugeben.

[2]Private Daten und E-Mails sind zu löschen. Für berufliche Daten und E-Mails ist nach Anweisung des Vorgesetzten vorzugehen.

[3]Kommt der Austretende diesen Pflichten nicht nach, kann das AFI oder die verantwortliche Lehrkraft die Informatikmittel räumen oder räumen lassen.

Art. 11

Nutzungsvorgaben

[1]Der Schulrat kann in Absprache mit dem AFI von Einschränkungen nach diesem Kapitel in begründeten Fällen Ausnahmen erlauben.

[2]Die Informatikstrategiekommission kann für die Nutzung von Informatikmitteln und für den sicheren Umgang mit diesen Richtlinien erlassen.

III. Einschränkungen für Internet und E-Mail-Dienste

Art. 12

Einschränkungen Internetnutzung

[1]Internetnutzungen und Zugriffe auf Websites sind untersagt, wenn sie die Arbeit beeinträchtigen, die Informatikstruktur belasten, mit Sicherheitsrisiken verbunden sind oder gegen das Recht oder die guten Sitten verstossen.

[2]Die Informatikstrategiekommission legt die untersagten Nutzungen und Zugriffe im Rahmen dieser Bestimmung in einer Liste fest, die den Mitarbeitern und Schülern in geeigneter Form mitzuteilen und zugänglich zu machen ist. Untersagte Nutzungen und Zugriffe können elektronisch gesperrt werden.

[3]Als untersagt gilt insbesondere der Zugriff auf Websites mit erotischem oder pornographischem Inhalt oder mit gewaltverherrlichendem, rassistischem, sexistischem oder extremistischem Inhalt.

Art. 13

Einschränkungen E-Mail-Dienste

[1]Die automatische Weiterleitung von E-Mails an externe E-Mail-Adressen ist untersagt.

[2]Das AFI kann die Anzahl der Adressaten und die Grösse der Anhänge aus betrieblichen oder technischen Gründen beschränken.

Art. 14

Ausnahmen

Der Schulrat kann von den Einschränkungen nach diesem Kapitel geschäftlich oder schulisch bedingte Ausnahmen erlauben.

IV. Internet- und Mailüberwachung

Art. 15

Aufzeichnung

[1]Das AFI ist berechtigt, die Verkehrsdaten der Internetzugriffe und des E-Mail-Verkehrs aufzuzeichnen.

[2]Im Falle von Internetzugriffen dürfen die Benutzernamen, die aufgerufenen Internetadressen, die Zeit und das Datum des Zugriffs sowie die Grösse der heruntergeladenen Dateien protokolliert werden.

[3]Im E-Mail-Verkehr dürfen Absender- und Empfängeradressen, Betreffzeile, Zeit und Datum der Übermittlung, Grösse der Mails und Bezeichnung sowie Grösse der Anhänge aufgezeichnet werden.

[4]Die Kontrolldaten werden unter Vorbehalt von Verdachtsfällen spätestens nach 12 Monaten gelöscht.

Art. 16

Melderecht

[1]Mitarbeiter, die Anzeichen für einen Verstoss gegen diesen Beschluss oder gegen eine strafrechtliche Norm wahrnehmen, sind berechtigt, dem Informatik-Sicherheitsbeauftragten Meldung zu erstatten.

[2]Das AFI und der Informatik-Sicherheitsbeauftragte sind berechtigt, die verantwortlichen Stellen über festgestellte Anzeichen zu informieren.

[3]Vorbehalten bleiben Strafanzeigen gemäss Art. 15 des Einführungsgesetzes zur Schweizerischen Strafprozessordnung (EG StPO).

Art. 17

Massnahmen bei Anzeichen für Verstösse

[1]Bei Anzeichen für Verstösse sind technische oder organisatorische Massnahmen zur Unterbindung weiterer Verstösse zu prüfen.

[2]Der Informatik-Sicherheitsbeauftragte kann bei Anzeichen für einen Verstoss in Absprache mit dem Schulrat eine personenbezogene Auswertung der Kontrolldaten durch das AFI anordnen.

[3]Der Informatik-Sicherheitsbeauftragte zeigt die Durchführung einer personenbezo-

genen Auswertung dem betroffenen Mitarbeiter und dem Schulrat an. Der Mitarbeiter darf Einsicht in die Daten und Resultate nehmen.

[4]Erhärtet sich der Verdacht aufgrund der Auswertung der greifbaren Daten nicht, ist die personenbezogene Auswertung abzubrechen. Die personenbezogenen Daten sind umgehend zu löschen. Der Informatik-Sicherheitsbeauftragte informiert den betroffenen Mitarbeiter und den Schulrat.

Art. 18

Verstösse

[1]Wird ein Verstoss festgestellt, informiert der Informatik-Sicherheitsbeauftragte die fehlbare Person, deren Vorgesetzten und den Schulrat.

[2]Personenbezogene Daten, die einen Verstoss dokumentieren, werden gesichert und im Personaldossier vermerkt.

Art. 19

Technische Probleme

[1]Der Informatik-Sicherheitsbeauftragte kann personenbezogene Auswertungen anordnen, soweit dies zur Ermittlung der Ursachen für technische Probleme oder zur Gewährleistung der Funktionsfähigkeit des Informatiksystems unerlässlich ist.

[2]Eine Anzeige an die betroffenen Personen ist nur notwendig, wenn Anzeichen bestehen, dass die Ursache für die technischen Probleme und die Gefährdung der Funktionsfähigkeit Verstösse gegen diesen Beschluss sind.

Art. 20

Andere Provider

[1]Wenn Internetzugänge nicht über das AINet laufen, können die Aufzeichnung und die Auswertung der Daten im Rahmen der vorstehenden Regelung dem Provider dieses anderen Netzes übertragen werden. Der Schulrat zeigt den Mitarbeitern an, wenn dies gemacht wird.

[2]Die Rechte und Pflichten der Mitarbeiter gemäss diesem Kapitel bleiben gleich.

V. Schlussbestimmungen

Art. 21

Sanktionen

[1]Im Falle von Verstössen gegen diesen Beschluss drohen neben strafrechtlichen Konsequenzen personalrechtliche Massnahmen und Schadenersatzansprüche.

[2]Das AFI kann im Einvernehmen mit dem Schulrat insbesondere

1. Informatikmittel entziehen oder die Nutzung einschränken;
2. den Internet- oder E-Mailzugang einschränken oder sperren;
3. Daten oder Programme blockieren oder löschen.

Art. 22

Ablösung bisherige Vorgaben

Dieser Beschluss löst die bisherigen Vorgaben für Informatiknutzer ab, insbesondere die Richtlinien für Informatikbenutzerinnen und -benutzer.

Art. 23

Inkrafttreten

Dieser Beschluss tritt auf den 1. August 2013 in Kraft.