

Sitzung vom 2. April 2014

Seite im Protokollbuch: 166

53	16.	Gemeindeorganisation
	16.01	Vorschriften, Verträge, Kreisschreiben
	31.	Schule
	31.01	Vorschriften, Verträge, Kreisschreiben
		Schule Lindau /
		Reglement für Informations- und Kommunikationstechnologie; Genehmigung

Öffentlich

Ausgangslage

Anlässlich der Sicherheitsüberprüfung auf der Gemeindeverwaltung wurden im Bereich Informations- und Kommunikationstechnologie einige Mängel festgestellt. Um diese zu beheben wurde ein Sicherheitskonzept erstellt.

Erwägungen

Da wir Einheitsgemeinde sind ist eine Ausweitung der Sicherheitsstandards auch im Bereich Schule erforderlich. Dies betrifft Mitarbeitende sowie Schülerinnen und Schüler.

Das vorliegende Reglement gibt die Nutzung der Informations- und Kommunikationstechnologie vor, im Speziellen den Gebrauch von E-Mail und Internet und die Verwendung mobiler Geräte. Gegenstand des Reglements ist zudem der verantwortungsvolle Umgang mit Informationen (insbesondere Personendaten).

Es bezweckt den Schutz der Informationen vor einem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität.

Die Schulpflege hat anlässlich ihrer Sitzung vom 17. März 2014 über das Reglement beraten und beschlossen, dieses dem Gemeinderat zur Genehmigung vorzulegen.

Beschluss

Der Gemeinderat, aufgrund der vorstehenden Ausführungen

beschliesst

1. Das vorliegende Reglement für Informations- und Kommunikationstechnologie der Schule Lindau wird genehmigt und per sofort eingeführt.
2. Die Umsetzung wird, gemäss Reglement, an die Schulleitungen delegiert.

3. Mitteilung durch Protokollauszug an:

- Schulpflege
- Schulleitungen
- Schulverwaltung
- IT-Verantwortlicher
- Homepage
- Akten

GEMEINDERAT LINDAU

Der Präsident:

Der Schreiber:

Bernard Hosang

Viktor Ledermann

versandt am:

Reglement für Informations- und Kommunikationstechnologie

Vorbemerkung

Entsprechend dem Grundsatz der Gleichstellung von Frau und Mann gelten alle Personen- und Funktionsbezeichnungen dieses Reglements ungeachtet der verwendeten Sprachform für beide Geschlechter.

1. Allgemeines

Dieses Reglement gibt die Nutzung der Informations- und Kommunikationstechnologie vor, im Speziellen den Gebrauch von E-Mail und Internet und die Verwendung mobiler Geräte. Gegenstand des Reglements ist zudem der verantwortungsvolle Umgang mit Informationen (insbesondere Personendaten).

Es bezweckt den Schutz der Informationen vor einem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität.

2. Ziel und Geltungsbereich

Diesem Reglement übergeordnet ist das Sicherheitskonzept der Gemeinde Lindau.

Das Reglement gilt für alle Mitarbeitenden und Schüler der Schule Lindau.

Als Mitarbeiter im Sinne dieses Reglements gelten alle fest oder temporär angestellten Mitarbeiter der Schule Lindau sowie die Behörden- und Kommissionsmitglieder.

3. Informations- und Kommunikationstechnologie

Die Informations- und Kommunikationstechnologie-Mittel (der Begriff umschliesst Internetdienste und die dazu nötige Hardware) sind sowohl für Unternehmen als auch Privatpersonen wichtige Instrumente für die Beschaffung und den Austausch von Informationen sowie für das Angebot und die Nutzung kommerzieller Dienstleistungen. Dabei sind die Rahmenbedingungen des Datenschutzes und der Informationssicherheit sowohl aus rechtlichen als auch sicherheitsrelevanten Gründen zwingend zu beachten.

Die Datenübermittlung erfolgt über äusserst komplexe Informationsverbindungen, die vom Anwender weder voraussehbar noch vorherbestimmbar sind. Datenverbindungen werden je nach der aktuellen Datenmenge automatisch auf verschiedenste Übertragungssysteme umgeleitet. Der Datenfluss ist in der Folge für den Anwender nicht kontrollierbar. Dennoch können die versandten Informationen von Dritten gelesen und manipuliert werden, sofern zu ihrem Schutz nicht besondere Massnahmen (z.B. Mailverschlüsselungsprogramme) ergriffen wurden. Der normale Mailverkehr – auch in der Schule Lindau – ist nicht verschlüsselt und daher gegenüber unbekanntem Dritten grundsätzlich als einsehbar zu betrachten.

4. Risiko

Der Gebrauch des Internets (auch über mobile Geräte) und insbesondere die Verwendung von Email-Systemen bergen in technischer, anwendungsmässiger sowie datenschutzrechtlicher Hinsicht teilweise erhebliche Risiken. Sie sind vom Laien schwer abschätzbar. Eine Schadensbehebung aufgrund der Missachtung von Sicherheitsvorschriften ist nicht nur zeitaufwändig sondern in

der Regel auch sehr kostenintensiv. Es gilt daher, diese Risiken durch die Einhaltung bestimmter Anwendungsvorschriften weit möglichst auszuschalten.

5. Zweck dieses Reglements

Das vorliegende Benützungsreglement von Informations- und Kommunikationstechnologie, nachstehend ‚Reglement‘ genannt, zeigt den sicheren Umgang mit elektronischen Werkzeugen auf und markiert den Wirkungsrahmen, innerhalb dessen sich die Mitarbeiter und Schüler der Schule Lindau gefahrlos bewegen können. Widerhandlungen gegen das Reglement begründen arbeits- und / oder strafrechtliche Konsequenzen. Die Erstellung dieses Reglements basiert auf den Vorgaben des Datenschutzbeauftragten.

6. Mitarbeitende

Die Mitarbeiter sind verpflichtet, die gesetzlichen Vorgaben und das Reglement zu beachten. Sie haben die Kenntnisnahme dieses Reglements unterschriftlich zu bestätigen.

Die Mitarbeiter sind verpflichtet, die ihnen zur Verfügung gestellten IKT Mittel recht- und zweckmässig einzusetzen und mit den Informationen, insbesondere mit Personendaten und besonderen Personendaten, sorgfältig umzugehen.

Die Mitarbeitenden melden alle sicherheitsrelevanten Ereignisse (Probleme, Vorfälle, Mängel usw.) sowie Schäden und Verlust von Hardware und Software dem IT-Verantwortlichen. Diese Stelle ist bei gravierenden Vorfällen verpflichtet, die Schulleitung zu informieren.

7. Internet

Alle Mitarbeiter der Schule Lindau nutzen das Internet an einem PC im Schulhaus. Ein Rechtsanspruch für diesen Internetzugang besteht nicht.

Das Internet ist grundsätzlich für Zwecke im Zusammenhang mit der Lehrtätigkeit, d.h. zur Erfüllung der zugewiesenen beruflichen Aufgaben, einzusetzen.

Der Internetanschluss kann bei Widerhandlungen gegen das Reglement jederzeit und ohne Vorankündigung gesperrt werden. Ausdrücklich vorbehalten bleibt das Recht, Webseiten mit ungeeignetem Inhalt (beispielsweise pornografisch, rassendiskriminierend, unethisch) oder mit erkennbaren Risiken (Virengefahr) zu sperren. Das Vorgehen im Ereignisfall erfolgt analog der Bestimmungen wie sie im Punkt „Missbrauch“ umschrieben sind.

8. Rechtsordnung

Unabhängig von den Bestimmungen in diesem Reglement gelten ohne weiteres u.a. folgende übergeordnete Vorschriften:

- Gesetz über die Information und den Datenschutz (IDG, LS 170.4)
- Verordnung über die Information und den Datenschutz (IDV, LS 170.41)
- Gemeindegesetz (GG, LS 131.1)
- Informatiksicherheitsverordnung (LS 170.8)
- Schweizerisches Strafgesetzbuch (StGB)
- Gemäss den Bestimmungen des Schweizerischen Strafgesetzbuches (StGB) sind das Abrufen und Publizieren folgender Inhalte auf Internet strafbar:
- Gewaltdarstellungen, Art. 135 StGB;

- Pornographie, Art. 197 Ziff. 1 + 3 StGB;
- Öffentliche Aufforderung zu Verbrechen oder zur Gewalttätigkeit, Art. 259 StGB;
- Strafbare Vorbereitungshandlungen, Art. 260bis 151 StGB;
- Kriminelle Organisation, Art. 260ter 153 StGB;
- Gefährdung der öffentlichen Sicherheit mit Waffen, Art. 260quater 154 StGB;
- Störung der Glaubens- und Kultusfreiheit, Art. 261 StGB;
- Rassendiskriminierung im Sinne von Art. 261bis 155 StGB;
- Anleitung oder Anstiftung zu strafbarem Verhalten oder dessen anderweitiger Förderung;
- Unerlaubte Glücksspiele.

Strafbare Handlungen im Internet sind grundsätzlich anzeigepflichtig (vgl. § 21 der kantonalen Strafprozessordnung StPO) und müssen umgehend dem IT-Verantwortlichen gemeldet werden.

9. Zugang – und Zugriffschutz

Die Mitarbeiter verhindern, dass Unbefugte Zutritt zu den Arbeitsräumlichkeiten haben. Halten sich externe Personen (z.B. Servicetechniker usw.) oder internes Personal (z.B. Reinigungspersonal, Behördenmitglieder) in den Räumlichkeiten auf, ist dafür zu sorgen, dass diese keinen unbefugten Zugang zu Informationen erhalten.

Der Arbeitsplatz ist bei Abwesenheiten so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Unterlagen und Datenträger offen zugänglich sind (Abschliessen des Schulzimmers, Sperren oder Herunterfahren des PCs).

Ausdrucke oder Kopien mit vertraulichen Informationen sind umgehend aus allgemeinen Geräten zu entfernen.

Die Mitarbeiter dürfen nur ihre persönlichen Benutzerkonten verwenden. Sie sind für den Zugriff auf ihr Konto verantwortlich.

Der Zugriff auf Personendaten, die nicht zur Aufgabenerfüllung benötigt werden, ist verboten.

Behördenmitglieder dürfen geschäftliche Daten nur dann auf privaten Geräten speichern, wenn eine dem Sicherheitsstandard der Schule Lindau entsprechende Zugangssicherung besteht. Es ist insbesondere verboten, Daten auf Geräten zu speichern, die auch anderen Familienmitgliedern oder Mitarbeitenden zugänglich sind.

Austretende Behördenmitglieder haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen (insbesondere besondere Personendaten), die ihnen zugänglich waren und die ausserhalb der Schule Lindau bearbeitet oder gespeichert wurden, unwiderruflich gelöscht (einfaches Löschen genügt nicht) oder der Verwaltung zurückgegeben wurden.

10. Passwörter

Passwörter sind vertraulich zu behandeln. Es ist verboten, eigene Benutzerkennungen und dazugehörige Passwörter unberechtigten Dritten zur Kenntnis zu bringen. Passwörter sind regelmässig - mindestens einmal jährlich - zu ändern.

Passwörter müssen mindestens acht Stellen lang sein und sollen eine Kombination von Klein- und Grossbuchstaben, Ziffern und Sonderzeichen enthalten.

Passwörter die einen Bezug zur eigenen Person aufweisen (z.B. Name, Name von Angehörigen, Geburtsdatum usw.), sind nicht erlaubt. Geschäftlich genutzte Passwörter dürfen nicht privat verwendet werden.

11. Datensicherung, Datenlöschung und Entsorgung von Informationsträgern

Geschäftsbezogene bzw. geschäftsrelevante Daten müssen auf Serverlaufwerken gespeichert bzw. archiviert werden.

Nicht mehr benötigte Daten müssen von Datenträgern (z.B. USB-Datenträger, Speicherkarten usw.) unwiederbringlich gelöscht werden. Personenbezogene Daten dürfen auf Mobilien Datenträgern nur mit Kennwortschutz gespeichert werden.

Nicht mehr benötigte Informationsträger (z.B. CD-ROM, USB-Datenträger usw.), die vertrauliche Informationen enthalten oder einmal enthielten, sind physikalisch zu vernichten (z.B. Shreddern).

12. Virenschutz

Die Mitarbeiter dürfen die Sicherheitssoftware (Virenschutz, Firewall usw.) nicht ausschalten, blockieren oder umkonfigurieren.

E-Mails mit unbekanntem Absender, verdächtigem Betreff oder unüblichem Inhalt sind im Hinblick darauf, dass sie von der Virenschutzsoftware nicht erkannte Viren enthalten könnten, vorsichtig zu behandeln. Deren Beilagen dürfen keinesfalls geöffnet werden. Jeder Verdacht auf Virenbefall muss sofort dem IT-Verantwortlichen gemeldet werden.

13. Hard- und Software im Schulnetzwerk

Der Einsatz von privaten Geräten ist im Einverständnis der Schulleitung gestattet.

Die Mitarbeiter dürfen auf schuleigenen Geräten keine Software und keine privaten Hardware-Erweiterungen, insbesondere keine Kommunikationseinrichtungen und externe Massenspeicher installieren bzw. anschliessen. Geschäftlich genutzte Speichermedien (z.B. Sticks) dürfen nur für geschäftliche Zwecke verwendet werden.

Die Mitarbeiter dürfen Informatiksysteme, die am Netzwerk angeschlossen sind, nicht gleichzeitig mit einem Netz oder System ausserhalb des Schul-Netzwerkes verbinden.

Nur der IT-Verantwortliche darf Geräte in die Reparatur oder zur Entsorgung geben. Dieser stellt sicher, dass keine schützenswerten Daten auf diesem Weg die Schule Lindau verlassen.

Änderungen an den Systemeinstellungen (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur vom IT-Verantwortlichen vorgenommen werden.

14. Mail Nutzung

Die Nutzung von E-Mail ist gegenüber der Verwendung von Faxgeräten und Briefpapier zu bevorzugen.

Dabei ist die Mailbox (elektronischer Briefkasten) möglichst oft, mindestens jedoch einmal pro Tag auf den Eingang von E-Mails zu kontrollieren. E-Mails sind innert nützlicher Frist zu beantworten.

15. Übertragung von vertraulichen Daten

Personendaten und / oder andere vertrauliche Daten dürfen nicht via E-Mail-System übertragen werden, da der Datenschutz bei der Übertragung nicht gewährleistet werden kann. Dies gilt nicht nur für E-Mail-Meldungen selbst, sondern auch für beigefügte Dokumente / Anlagen (so genannte Attachements).

16. Private Nutzung

Die Nutzung des Internets sowie des E-Mail-Systems für private Zwecke ist zulässig, sofern dabei das Netzwerk nicht beeinträchtigt wird. Diese Privatanwendungen während der Arbeitszeit sind auf ein Minimum zu beschränken.

Private E-Mails müssen entweder gelöscht oder in einem persönlichen Ordner mit der Bezeichnung „PRIVAT“ abgelegt werden.

Verboten sind:

- Die elektronische Übermittlung von Programmen oder Programmteilen inkl. Video- und / oder Sounddateien.
- Der Zugriff auf Informationen mit widerrechtlichem, urheberrechtsverletzendem, rassistischem, beleidigendem, pornografischem oder herabwürdigendem Inhalt u. dergleichen oder die Verbreitung / Weiterleitung solcher Inhalte.

17. Downloads

Das Herunterladen von Daten und Dateien ist nur zulässig, wenn es sich um schulrelevante Informationen handelt und deren Ursprung bekannt ist. In Zweifelsfällen ist der IT-Verantwortliche zu kontaktieren.

Ausdrücklich verboten ist das Herunterladen und/oder Installieren von Programmen oder Programmteilen.

18. Einsatz mobiler Geräte ausserhalb der Schulanlage

Die Nutzung privater mobiler Geräte über die Kabelgebundene Verbindung (LAN) ist aus sicherheitstechnischen Gründen nicht gestattet.

Der Zugriff auf das Internet über ein separates WLAN ist möglich. Die Zugangsdaten sind beim IT-Verantwortlichen der Schuleinheit einzuholen.

19. Meldepflicht von ausserordentlichen Ereignissen

Ein für den Anwender nicht erklärbares Systemverhalten, nicht nachvollziehbarer Verlust von Daten bzw. Datenveränderungen, unaufgeforderte Verfügbarkeit von gesperrten Diensten, Verdacht auf Missbrauch der eigenen Benutzererkennung etc. sind umgehend dem IT-Verantwortlichen melden.

20. Hinweis auf Kontrollen und Protokollierung

Es wird ausdrücklich darauf hingewiesen, dass das Surf-Verhalten der einzelnen Anwender im In-

ternet bis zum Ausgangspunkt (PC-Arbeitsplatz, mobile Geräte) zurückverfolgt werden kann.

Durch Mitarbeiter aufgerufene Websites werden automatisiert nach rechtswidrigen Inhalten gescannt.

Das IT-System erstellt automatisiert Zugriffsprotokolle unter Berücksichtigung der Daten-Schutz Gesetzgebung des Kantons Zürich, insbesondere betreffend des Schutzes der Privatsphäre. Die Protokollinformationen dienen dabei ausschliesslich dem Zweck der Datenschutzüberprüfung, der IT-Revision, Sicherung von Daten sowie der Gewährleistung eines störungsfreien IT-Betriebes. Es erfolgt keine personenbezogene Auswertung / Überwachung für Verhaltens- und / oder Leistungskontrollen.

21. Missbrauch

Wird ein Missbrauch auf Grund der automatischen Protokollierung und dem Resultat von Auswertungen festgestellt, informiert der IT-Verantwortliche die Schulleitung und den Sicherheitsvorstand der Gemeinde. In einem solchen Fall kann der Sicherheitsvorstand der Gemeinde, nach Information des betroffenen Mitarbeiters durch die Schulleitung, eine personenbezogene Überwachung anordnen.

22. Sanktionen bei Widerhandlung gegen dieses Reglement

Verstösse gegen die Bestimmungen dieses Reglements oder generell widerrechtliches Verhalten im Zusammenhang mit der Anwendung der Internettechnologie der Schule Lindau können nach den Bestimmungen des Personalrechtes und des Strafrechtes geahndet werden.

23. Schüler

Für die Schüler werden Regeln für den Umgang und die Handhabung der ihnen zur Verfügung gestellten Mittel erstellt, sowie die Verbindlichkeit und Vorgehensregelung bei Nichteinhaltung festgelegt.

Das Erstellen der Regeln ist Sache der einzelnen Schuleinheit. Es soll von den Schulleitungen stufengerecht erstellt werden.

24. Schlussbemerkung

Dieses Reglement wird allen Mitarbeitern im Sinne einer Dienstanweisung durch die Schulleitung zugestellt. Die Anerkennung des Inhaltes wird schriftlich auf einem separaten Formular, welches in den Personalakten aufbewahrt wird, bestätigt.

Die Abgabe dieses Reglements und das Unterzeichnen des separaten Formulars obliegen der Schulleitung.

25. Inkrafttreten

Dieses Reglement hat der Gemeinderat mit Beschluss vom 2. April 2014 genehmigt und wird per sofort in Kraft gesetzt.

Änderungen sind mit Beschluss des Gemeinderates jederzeit möglich.