ZÜRCHER LEHRBETRIEBSVERBAND ICT

Inhaltsverzeichnis

ZÜRCHER LEHRBETRIEBSVERBAND ICT

Hausordnung

1. Alle Kursteilnehmenden und Mitarbeitenden sind verpflichtet, die Geschäftsleitung in der Handhabung der Hausordnung zu unterstützen. Für das Einhalten der Hausordnung ist die Geschäftsleitung verantwortlich. Besondere Vorkommnisse sind der Geschäftsleitung zu melden.

2. Die Unterrichtszeit ist einzuhalten. Bei Nichterscheinen des Kursleitenden ist im Sekretariat 10 Minuten nach Kursbeginn durch die Klasse Mitteilung zu machen. Abweichungen sind nur nach Absprache mit der Schulleitung zulässig.

3. Das Auftreten in Bezug auf Kleidung, Sprache und Verhalten richtet sich nach den Gepflogenheiten des Wirtschaftslebens. Es werden keine stark auffallenden „Styles" (zum Beispiel Hip-Hop oder Skater), Hosen tief im Schritt, sichtbare Unterhosen, Basketball Shirts, bauchfreie Tops, Hotpants, Flipflops toleriert. Innerhalb des ganzen Gebäudes werden keine Kopfbedeckungen getragen. Es werden keine rassistischen, sexistischen oder gewaltbetonten Bilder oder Sprüche (schriftlich oder mündlich) toleriert.

4. Das Arbeiten (auch im Unterricht) darf nicht durch Lärm in den Gängen und im Treppenhaus gestört werden. Das Treppenhaus ist kein Pausenaufenthaltsraum. Am Arbeitsplatz ist grösstmögliche Rücksicht auf die andern Mitarbeitenden zu nehmen, unnötiger Lärm ist zu vermeiden

5. Die Räumlichkeiten des ZLI sind kein öffentlicher Raum und der Aufenthalt von Drittpersonen ist nicht gestattet.

6. In sämtlichen Räumen ist auf Ordnung und Reinlichkeit zu achten. Jeden Abend sind Monitore und PCs ausgeschaltet, sind die Tische abgeräumt, stehen die Stühle ordentlich am Tisch, sind die PET-Flaschen entsorgt, ist das Papier (Ausdrucke) in der Sammelstelle, sind die Fenster geschlossen und sind die Lichter ausgeschaltet.

7. Alle Räumlichkeiten und Einrichtungen sind sorgfältig zu benutzen. Schäden sind dem Sekretariat zu melden. Missbrauch und mutwillige Beschädigungen werden geahndet und Fehlbare haften für Schäden.

8. Integrierter Bestandteil der Hausordnung sind das Betriebskonzept Videoüberwachung, die IT-Nutzungsrichtlinie sowie die WLAN Nutzungsbedingungen. Verstösse werden geahndet.

9. Es ist nicht erwünscht, dass die Kursteilnehmenden die Pausen in den Ausbildungsräumen verbringen. Die Kursleitenden sind angewiesen, die Kursteilnehmenden während der Pausen und am Mittag aus dem Zimmer zu schicken.

10. Das Mitführen und/oder das Konsumieren von Suchtmitteln (insbesondere Alkohol (inkl. Alcopops), Drogen (z.B. Haschisch)) ist auf dem ganzen ZLI Areal untersagt. Das ganze Haus ist rauchfreie Zone.

11. Der ZLI stellt den Teilnehmenden keine Parkplätze zur Verfügung.

12. Fahrräder, Motorfahrräder und Motorräder sind an den besonders bezeichneten Orten abzustellen.

13. Für die Verpflegung stehen Essbereiche zur Verfügung. Es ist verboten an den Arbeitsplätzen zu essen. Getränke dürfen nur in verschliessbaren Behältern mit Drehverschluss an die Arbeitsplätze genommen werden.

14. Fundgegenstände sind dem Kursleitenden oder im Sekretariat abzugeben; sie können vom Besitzer dort abgeholt werden.

15. Diebstähle sind sofort dem Sekretariat zu melden. Der ZLI lehnt jede Haftung ab.

16. Der Teilnehmende an ZLI Dienstleistungen haftet für die von ihm verursachten Schäden; weitere rechtliche Schritte bleiben vorbehalten. Beschädigungen sind dem Kursleitenden oder im Sekretariat zu melden. Wer in den Ausbildungsanlagen Verunreinigungen (z.B. Rauchen an verbotenen Orten) verursacht, hat für den Kontroll- und Reinigungsaufwand aufzukommen. Der Mindestbetrag für eine Kontrolle und/oder Reinigung durch Dritte beträgt CHF 200.-. Sämtliche Kosten für mutwillig oder fahrlässig ausgelöste Alarme gehen zu Lasten des Verursachenden.

17. Auf dem gesamten ZLI Areal darf nicht für geschäftliche, konfessionelle oder partei- respektive vereinspolitische Zwecke geworben werden. Die Geschäftsleitung entscheidet über die Zulassung von Bekanntmachungen, über die Durchführung von Sammlungen, Fachvorträgen und Ausstellungen. Die Benutzung des Anschlagsbretts wird durch die Geschäftsleitung geregelt.

18. Verstösse gegen die Hausordnung werden geahndet.

19. Die Geschäftsleitung hat dafür zu sorgen, dass die Hausordnung allen Mitarbeitenden, Kursleitenden und Kursteilnehmenden bekannt gegeben wird.

20. Diese Hausordnung tritt auf den 17. Juli 2017 in Kraft.

Betriebskonzept Videoüberwachung

Einführung

Dieses Betriebskonzept wurde gemäss den Publikationen über die Videoüberwachung auf der Website «Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (EDÖB)» (https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/technologien/videoueberwachung.html) erstellt.

Zweck

Die Videoüberwachung dient dem Schutz von Personen und Sachen. Insbesondere folgende Ziele sollen erreicht werden:

- Weniger Littering und Vandalismus im Gebäude
- Personen fühlen sich sicher im Gebäude
- Mögliche Beweise oder Indizien bei Diebstahl, Einbrüchen oder Sachbeschädigung aller Art

Organisation

Verantwortliche Stelle: Die verantwortliche Stelle ist die Geschäftsleitung ZLI. Diese sorgt für die regelmässige Überprüfung und Umsetzung der Datenschutzbestimmungen.

Ziele: Bei Einbrüchen, Sachbeschädigungen, Bedrohung der Gesundheit oder anderen groben Verstössen sollen die Täter unter Verwendung der Videoaufzeichnungen identifiziert werden oder der Polizei mögliche Indizien für die Überführung der Täter liefern.

Überwachungsbereich: Im Erdgeschoss wird der Gang Nord und die Cafeteria und im 1. Obergeschoss die Gänge, die Aufenthalte 1 bis 3 sowie der Projektraum überwacht. Im Anhang A sind in den Grundrissen der Geschosse die Überwachungsbereiche rot ausgewiesen.

Überwachungszeiten: Die Überwachungsbereiche werden dauernd überwacht. Die Aufzeichnungen startet sobald Bewegung im Aufnahmefeld festgestellt wird.

Überwachungsart: Die Überwachung zeichnet die Videos passiv auf. Es wird Bildmaterial aber keine Audiodaten aufgezeichnet. Bereiche ausserhalb des Überwachungsbereichs werden mit Privacy Filtern unkenntlich gemacht.

Technik: Die Kameras übermitteln die Bilder über Kabelnetzwerk an einen Server, welcher die Aufzeichnungen auf eine Harddisk speichert.

Auswertungen: Die Auswertung der Videoaufzeichnungen erfolgt nach aussergewöhnlichen Vorkommnissen durch die Geschäftsleitung ZLI, Mitarbeitende in der Technik und/oder durch die Polizei. Zugriffe auf die Videoaufzeichnungen werden protokolliert.

Aufbewahrungszeit: Die Videoaufzeichnungen werden in der Regel nach 30 Tagen automatisch gelöscht.

Datenschutzvereinbarung: Falls die Videoüberwachung durch eine andere als die verantwortliche Stelle durchgeführt wird, ist eine entsprechende Datenschutzvereinbarung nötig.

Betrieb

Hinweisschilder: Gut sichtbare Hinweisschilder bei den Eingängen weisen auf die Videoüberwachung hin.

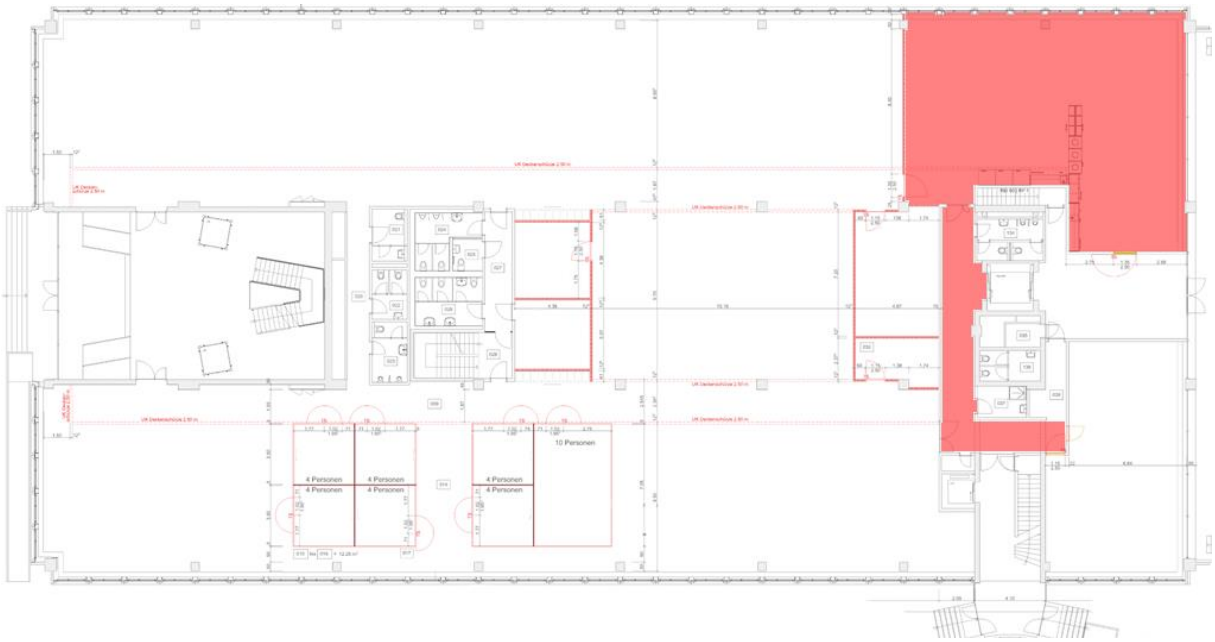
Serverstandort: Der Server ist in einem Rack im Serverraum ZLI untergebracht. Physikalischen Zutritt zum Server hat die Geschäftsleitung ZLI und Mitarbeitende in der Technik.

Aufbewahrung, Weitergabe Videoaufzeichnung: Die Videoaufzeichnungen sind ausschliesslich auf der Harddisk des Servers vorhanden. Wird zwecks Beweisführung eine DVD oder ein ähnliches Medium erstellt, soll dieses sofort der Polizei übergeben werden. Eine Weitergabe an die Strafuntersuchungsbehörden ist nur im Rahmen der Einleitung eines Strafverfahrens möglich.

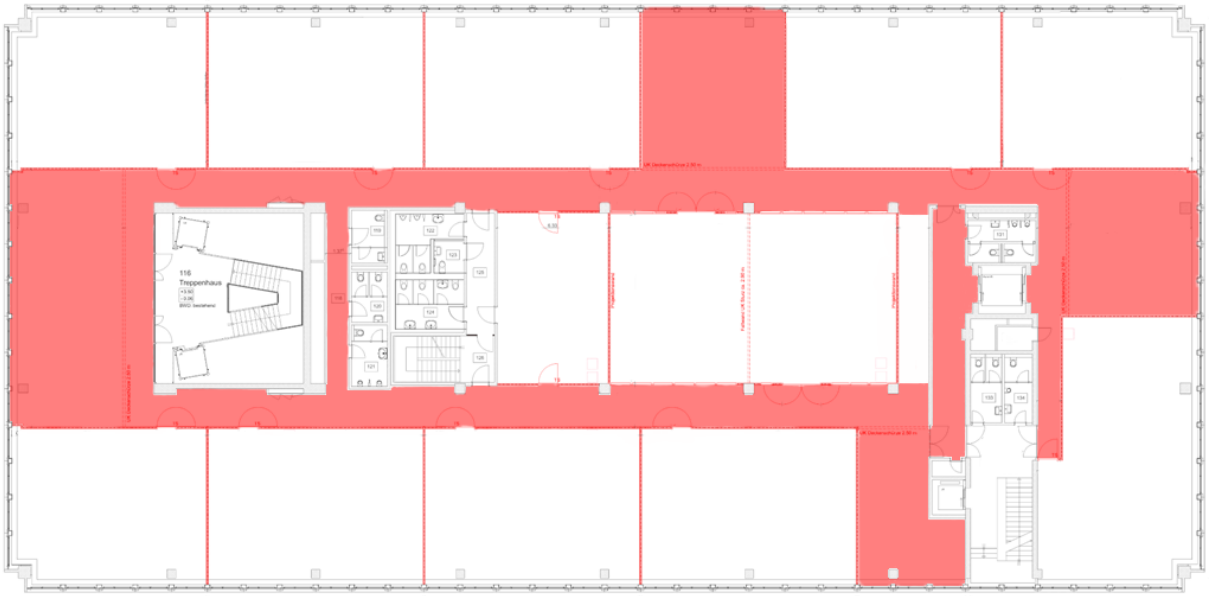
Anhang A: Überwachter Bereich im ZLI

Die in den Grundrissen rot markierte Bereiche werden überwacht.

Erdgeschoss:



1. Obergeschoss



IT-Nutzungsrichtlinie

Gegenstand der Richtlinie

Diese Richtlinie regelt in verbindlicher Weise die Nutzung der Informatikmittel des Zürcher Lehrbetriebsverband ICT (ZLI) (nachfolgend "ZLI", "Betreiber" oder "Systembetreiber"), die entweder durch den ZLI zur Verfügung gestellt werden oder durch Mitarbeitende oder Auszubildende mit eigenen Geräten genutzt werden.
Diese Nutzungsrichtlinie ist ein integraler Bestandteil des Arbeits-, Ausbildungs- oder Mandatsvertrags sowie der Ausbildungsvereinbarungen mit Auszubildenden.
Wegen der besseren Lesbarkeit wird in diesem Dokument ausschliesslich die männliche Form verwendet. Die weibliche Form ist selbstverständlich immer miteingeschlossen.

Ziele der Richtlinie

Die IT Nutzungsrichtlinie …

- orientiert sich an den gesetzlich und vertraglich festgelegten Aufgaben des Ausbildungszentrums;
- stellt Grundregeln für einen ordnungsgemässen Betrieb der IT-Infrastruktur auf;
- weist auf die zu wahrenden Rechte Dritter (z.B. bei Softwarelizenzen, Auflagen der Netzbetreiber, Datenschutzaspekte) hin;
- verpflichtet die Benutzer zu korrektem Verhalten und zum ökonomischen Gebrauch der angebotenen Ressourcen;
- klärt über eventuelle Massnahmen des Betreibers bei Verstössen gegen die Benutzungsrichtlinien auf.

Geltungsbereich

Diese Richtlinie richtet sich an alle Kursteilnehmende, Kursleitende und Mitarbeitende sowie Gäste im ZLI.
Als Informatikmittel des ZLI gelten: Hardware wie z.B. PC, Notebooks, Tablets, Mobiles, Server, Netzwerke, Telekommunikationseinrichtungen, WLAN, Applikationen, Moodle, Drucker, Multimediageräte sowie Software (Betriebssysteme, Programme und Daten).
Diese Richtlinie findet auch auf private Geräte Anwendung, wenn Sie mit dem ZLI Netzwerk verbunden werden.

Bring your own device (BYOD)

Der ZLI ermöglicht die Nutzung der ICT-Infrastruktur mit den eigenen privaten Endgeräten (Notebooks, Tablets, Mobiles) als BYOD (Bring your own device) Anwendung. Nur in Ausnahmefällen werden den Kurteilnehmenden und Kursleitenden betriebseigene Endgeräte zur Verfügung gestellt.
Bei der Verwendung von eigenen Endgeräten sind diese zwingend durch ein Passwort zu schützen. Private und geschäftliche Daten sind strikt zu trennen. Geschäftliche Daten dürfen nur auf den zugewiesenen Speicherorten und keinesfalls auf den privaten Geräten gespeichert werden.
Mit der Verwendung von privaten Geräten unter der BYOD Anwendung gestattet der Nutzer dem ZLI auf das Gerät online zuzugreifen oder stellt dieses der IT zur Verfügung für Geräteüberprüfungen, Fernwartung, Sicherheitsupdates, Datenlöschungen oder zur Prüfung der Einhaltung dieser Weisung. Falls ein Zugriff ausserhalb des geschäftlichen Teils notwendig wird, ist in jedem Fall vor jedem Zugriff die Einwilligung einzuholen.
Der Nutzer ist verpflichtet, seine Geräte und Softwareanwendungen auf dem neusten Stand zu halten und laufend zu aktualisieren sowie einen aktuellen Malware-Schutz zu verwenden. Es dürfen auf den privaten Geräten nur lizenzierte Software oder Applikationen verwendet werden. Es wird kein technischer Support für private Geräte angeboten.
Ein allfälliger Diebstahl oder Verlust ist sofort zu melden, damit die Zugriffe auf die Netzwerke des ZLI gesperrt werden können.
Es erfolgt grundsätzlich keine Entschädigung für die Nutzung der eigenen Geräte. Ausnahmen für festangestellte Mitarbeitende sind im Personalreglement geregelt.

Formale Benutzungsberechtigung

Wer ICT-Ressourcen benutzen will, bedarf einer formalen Benutzungsberechtigung des zuständigen Systembetreibers. Ausgenommen sind Dienste, die für anonymen Zugang eingerichtet sind (z.B. Informationsdienste, Bibliotheksdienste, kurzfristige Gastkennungen bei Tagungen).
Der Antrag auf eine formale Benutzungsberechtigung soll folgende Angaben enthalten:

- Systeme, für welche die Benutzungsberechtigung beantragt wird
- Antragsteller: Name, Adresse, Telefonnummer und evtl. Zugehörigkeit zu einer organisatorischen Einheit
- Überschlägige Angaben zum Zweck der Nutzung, beispielsweise „Berufslehre für Erwachsene"
- die Erklärung, dass der Benutzer die Benutzungsrichtlinien anerkennt
- Einträge für Informationsdienste

Weitere Angaben darf der Systembetreiber nur verlangen, soweit sie zur Entscheidung über den Antrag erforderlich sind.
Über den Antrag entscheidet der zuständige Systembetreiber. Er kann die Erteilung der Benutzungsberechtigung vom Nachweis bestimmter Kenntnisse über die Benutzung der Anlage abhängig machen.
Die Benutzungsberechtigung darf versagt werden, wenn

- nicht gewährleistet erscheint, dass der Antragsteller seinen Pflichten als Nutzer nachkommen wird.
- die Kapazität der Anlage, deren Benutzung beantragt wird, wegen einer bereits bestehenden Auslastung für die beabsichtigten Arbeiten nicht ausreicht.
- das Vorhaben nicht mit den Zwecken des Ausbildungszentrums vereinbar ist.
- die Anlage für die beabsichtigte Nutzung offensichtlich ungeeignet oder für spezielle Zwecke reserviert ist.
- die zu benutzende Anlage an ein Netz angeschlossen ist, das besonderen Datenschutzerfordernissen genügen

muss und kein sachlicher Grund für diesen Zugriffswunsch ersichtlich ist.
- zu erwarten ist, dass durch die beantragte Nutzung andere berechtigte Nutzungen in nicht angemessener Weise gestört werden.
- die zu verrichtenden Arbeiten nicht im Zusammenhang mit dem beantragten Nutzen stehen.

Allgemeine Grundsätze der Nutzung

Die ICT-Ressourcen dürfen nur für betriebliche Zwecke genutzt werden. Eine rein private Nutzung kann nur auf Antrag und gegen Entgelt gestattet werden.
Der Benutzer ist verpflichtet, darauf zu achten, dass er die vorhandenen Betriebsmittel (Arbeitsplätze, CPU-Kapazität, Plattenspeicherplatz, Leitungskapazitäten, Peripheriegeräte und Verbrauchsmaterial) verantwortungsvoll und ökonomisch sinnvoll nutzt. Der Benutzer ist verpflichtet, Beeinträchtigungen des Betriebes, soweit sie vorhersehbar sind, zu unterlassen und nach bestem Wissen alles zu vermeiden, was Schaden an der ICT-Infrastruktur oder bei anderen Benutzern verursachen kann.

- Zuwiderhandlungen können Schadenersatzansprüche begründen
- Der Benutzer hat jegliche Art der missbräuchlichen Benutzung der ICT-Infrastruktur zu unterlassen
- Er ist insbesondere dazu verpflichtet
  - ausschliesslich mit Benutzerkennungen zu arbeiten, deren Nutzung ihm gestattet wurde; die Weitergabe von Kennungen und Passwörtern ist grundsätzlich nicht gestattet.
  - den Zugang zu den ICT-Ressourcen durch ein geheim zuhaltendes Passwort oder ein gleichwertiges Verfahren zu schützen.
  - Vorkehrungen zu treffen, damit unberechtigten Dritten der Zugang zu den ICT-Ressourcen verwehrt wird; dazu gehört es insbesondere, primitive, naheliegende Passwörter zu meiden, die Passwörter öfter zu ändern und das Logout nicht zu vergessen.

Der Benutzer trägt die volle Verantwortung für alle Aktionen, die unter seiner Benutzerkennung vorgenommen werden, und zwar auch dann, wenn diese Aktionen durch Dritte vorgenommen werden, denen er zumindest fahrlässig den Zugang ermöglicht hat.
Der Benutzer ist des Weiteren verpflichtet,

- bei der Benutzung von Software (Quellen, Objekte), Dokumentationen und anderen Daten die gesetzlichen Regelungen (Urheberrechtsschutz, Copyright) einzuhalten.
- sich über die Bedingungen, unter denen die zum Teil im Rahmen von Lizenzverträgen erworbene Software, Dokumentationen oder Daten zur Verfügung gestellt werden, zu informieren und diese Bedingungen zu beachten.
- insbesondere Software, Dokumentationen und Daten, soweit nicht ausdrücklich erlaubt, weder zu kopieren noch weiterzugeben noch zu anderen als den erlaubten, insbesondere nicht zu gewerblichen Zwecken zu nutzen.

Zuwiderhandlungen können Schadenersatzansprüche begründen.
Selbstverständlich darf die ICT-Infrastruktur nur in rechtlich korrekter Weise genutzt werden. Es wird ausdrücklich darauf hingewiesen, dass insbesondere folgende Verhaltensweisen und Sachverhalte unter Strafe gestellt sind:

- Ausforschen fremder Passworte, Ausspähen von Daten
- unbefugtes Verändern, Löschen, Unterdrücken oder Unbrauchbarmachen von Daten
- Computersabotage und Computerbetrug
- die Verbreitung von Propagandamitteln verfassungswidriger Organisationen oder mit rassistischem Gedankengut
- die Verbreitung aller Formen von Pornographie
- Abruf oder Besitz von Dokumenten mit Kinderpornographie
- Ehrdelikte wie Beleidigung, Verleumdung
- sexistisches, rassistisches oder gewaltbetontes Material zu besitzen und zu verbreiten
- Widerrechtliches Bereitstellen (Upload) und Verbreiten von urheberrechtlich geschützten Werken jeglicher Art (insbesondere Filme, Musik und Fotos).

Der Systembetreiber behält sich strafrechtliche Schritte sowie zivilrechtliche Ansprüche vor.
Dem Benutzer ist es untersagt, ohne Einwilligung des zuständigen Systembetreibers

- Eingriffe in die Hardware-Installation vorzunehmen.
- die Konfiguration der Betriebssysteme oder des Netzwerkes zu verändern.

Die Berechtigung zur Installation von Software ist in Abhängigkeit von den jeweiligen örtlichen und systemtechnischen Gegebenheiten gesondert geregelt.
Der Benutzer ist verpflichtet, ein Vorhaben zur Bearbeitung personenbezogener Daten vor Beginn mit dem Systembetreiber abzustimmen. Davon unberührt sind die Verpflichtungen, die sich aus Bestimmungen des Bundesgesetzes über den Datenschutz ergeben.
Dem Benutzer ist es untersagt, für andere Benutzer bestimmte Nachrichten zur Kenntnis zu nehmen und/oder zu verwerten.
Der Benutzer ist verpflichtet,

- die vom Systembetreiber zur Verfügung gestellten Leitfäden zur Benutzung zu beachten.
- im Verkehr mit Rechnern und Netzen anderer Betreiber deren Benutzungs- und Zugriffsrichtlinien einzuhalten.

Internet und WLAN

Der ZLI stellt ein WLAN mit einem personifizierten Zugang für den Zugriff auf das Internet und auf interne Ressourcen bereit. Es gelten die separaten WLAN-Nutzungsbedingungen.
Jeder Benutzer hat das Recht, das Internet zu benützen. Die Internetdienste dürfen nur betrieblich oder für schulische Zwecke genutzt werden. Eine geringfügige Privatnutzung ist erlaubt, sofern dadurch keine negativen Auswirkungen auf die Arbeitsleistungen auftreten.

Der Internetzugang kann für Kursteilnehmende und Kursleitende eingeschränkt werden. Es ist verboten, dies zu umgehen. Bei der Nutzung des Internets mit Informatikmitteln des ZLI gelten die gesetzlichen Bestimmungen wie beispielsweise Jugendschutz, Urheberrecht, Strafnorm gegen Rassismus.
Das Kopieren von Daten vom Internet auf den lokalen PC oder in der Gegenrichtung (z.B. Mail oder FTP) durch Kursteilnehmende bedarf der Zustimmung des Kursleitenden. Die Verwendung von Message-Diensten und Chatrooms (z.B. IRC, MS Messenger, ICQ usw.) sind verboten. Der Internet-Zugriff wird überwacht, protokolliert und ausgewertet. Bei Hinweisen auf einen Missbrauch oder Verstoss gegen die Nutzungsbedingung wird die Auswertung personenbezogen vorgenommen.

Nutzung der E-Mail Dienste

Der ZLI stellt nach Bedarf einen persönlichen E-Mail Account zur Verfügung. Die zugewiesene persönliche E-Mail-Adresse soll nicht für private Zwecke benutzt werden. Der Empfang und Versand von E-Mails mit privaten Inhalten über die Kommunikationssysteme des ZLI wird lediglich toleriert und ist nicht ausdrücklich erlaubt. Private E-Mails sind mit „PRIVAT" zu kennzeichnen und in einem separaten Ordner „PRIVAT" abzulegen. Diese privaten E-Mails sind spätestens beim Austritt durch den Benutzer zu löschen. Die vom ZLI zur Verfügung gestellte E-Mail-Adresse darf nicht zu privaten Zwecken als Identifikation, Kontaktkoordinate oder zur Registrierung für Zugänge zu Diensten oder Kommunikationsplattformen, insbesondere sozialen Netzwerken verwendet werden.
Benutzer mit einer von der ZLI zur Verfügung gestellten E-Mail-Adresse, anerkennen die Tatsache, dass in Situationen von technischen, administrativen, organisatorischen Notsituationen der Zugriff auf eines oder alle Postfächer notwendig werden kann. Der direkte Zugriff durch Vorgesetzte auf das E-Mail-Konto einer Mitarbeiterin oder eines Mitarbeiters ist grundsätzlich nicht erlaubt. Vorgesetzte dürfen von Mitarbeitenden jedoch Rechenschaft über den dienstlichen E-Mail-Verkehr verlangen und bei Anhaltspunkten für Pflichtverletzungen auch personalrechtliche Massnahmen ergreifen, die allenfalls zu einer Einsichtnahme in ein E-Mail-Konto führen können. Bei Abwesenheiten ist ein Stellvertreter mit abgestufter Berechtigung zur Einsicht und Weiterbearbeitung der eingehenden geschäftlichen E-Mails zu definieren. Die als «PRIVAT» gekennzeichneten E-Mails sind für den Stellvertreter nicht sichtbar. Bei unerwarteten längeren Abwesenheiten infolge Krankheit oder Unfall darf die Informatik die Stellvertretungsfunktion aktivieren.
Über Datensicherungen und Archivierungssysteme werden sämtliche E-Mails permanent / langfristig ungeachtet ihres Inhalts gesichert. Die Kapazität der Postfächer ist fest vorgegeben. Die Transportgrösse von E-Mails ist auf max. 20 MB begrenzt.
E-Mail-Nachrichten mit unbekanntem Absender, die dazu auffordern, einen Link anzuklicken oder ein angehängtes Dokument zu öffnen, müssen ignoriert und gelöscht werden. Dasselbe gilt für Ketten-E-Mails. Im Zweifelsfall ist mit der IT Rücksprache zu halten. Bei E-Mail Nachrichten von bekannten Absendern mit ungewöhnlichen Inhalten, die dazu auffordern einen Link anzuklicken oder mit ungewöhnlichen anhängen, die dazu auffordern angehängtes Dokumente zu öffnen dürfen nicht ohne Rücksprache und Überprüfung, dass es sich nicht um ein sogenanntes Phising Mail handelt, geöffnet werden. Mails, die dazu auffordern, sensitive Daten wie Online-Banking-Informationen, Kreditkartennummern oder Passwörter preiszugeben (= Phishing Mails), müssen ebenfalls ignoriert und gelöscht werden.
Das direkte Umleiten der E-Mail von der ZLI Adresse auf eine externe Mailadresse um auf E-Mails ausserhalb Zugriff zu haben, ist nicht erlaubt.
Der Mitarbeiter ist dafür verantwortlich, externe Absender zu informieren, dass private E-Mails als solche zu kennzeichnen sind, ansonsten sie durch den Stellvertreter eingesehen werden können.

Aufgaben, Rechte und Pflichten der Systembetreiber

Jeder Systembetreiber muss über die erteilten Benutzungsberechtigungen eine Dokumentation führen. Die Unterlagen sind nach Auslaufen der Berechtigung mindestens zwei Jahre aufzubewahren.
Der Systembetreiber trägt in angemessener Weise, insbesondere in Form regelmässiger Stichproben, zum Verhindern bzw. Aufdecken von Missbrauch bei. Daraus ergeben sich die nachfolgend aufgeführten Rechte bzw. erlaubt folgende Massnahmen:

- Die Aktivitäten der Benutzer dürfen dokumentiert und ausgewertet werden, soweit dies zu Zwecken der Abrechnung von IT-Ressourcen, der Ressourcenplanung, der Überwachung des Betriebes oder der Verfolgung von Fehlerfällen und Verstössen gegen die Benutzungsrichtlinien sowie gesetzlichen Bestimmungen dient.
- Bei Verdacht auf Verstösse gegen die Benutzungsrichtlinie oder gegen strafrechtliche Bestimmungen darf der Systembetreiber unter Beachtung des Vieraugenprinzips und der Aufzeichnungspflicht in Benutzerdateien und Mailboxen Einsicht nehmen oder die Netzwerknutzung durch den Benutzer mittels z.B. Netzwerk-Sniffer detailliert protokollieren.
- Die nicht personenbezogene (anonyme) Auswertung der Logfiles durch die Geschäftsleitung oder Informatik ist jederzeit ohne vorherige Ankündigung zulässig. Sie bezweckt die statistische Auswertung nach systemspezifischen Kriterien (Beispiele: meistbesuchte Websites, beanspruchte Bandbreite, grösste Downloads, Anzahl versandter Mails).
- Pseudonyme Auswertungen der Logfiles können auf Anordnung der Geschäftsleitung oder Informatik stichprobenartig, aber nicht permanent, durchgeführt werden. Die Schulangehörigen sind über den Zeitraum der pseudonymen Auswertungen vorher in geeigneter Form zu orientieren. Pseudonyme Auswertungen bezwecken eine Auswertung der Logfiles nach pseudonymisierten, be-

stimmbaren Personen. (Beispiele: meistbesuchte Websites nach Nutzergruppen, Anzahl versandter Mails nach Nutzergruppen während der Auswertungsperiode.) Die Identität der von der pseudonymen Auswertung betroffenen Personen darf nicht leicht zu rekonstruieren sein.

- Falls im Rahmen anonymer und/oder pseudonymer Auswertungen Missbräuche festgestellt werden oder ein Missbrauchsverdacht besteht, so können die Logfiles namentlich personenbezogen ausgewertet werden. Wenn sich der Missbrauchsverdacht nicht erhärtet, so wird die namentliche personenbezogene Auswertung der Logfiles umgehend eingestellt.
- Im Falle einer festgestellten oder vermuteten Straftat werden die Logfiles separat gesichert. Die Geschäftsleitung oder Informatik wird gegebenenfalls disziplinar- und/oder strafrechtliche Schritte einleiten.
- Im Fall einer personenbezogenen Auswertung von Logfiles werden die davon betroffenen Personen im Nachhinein informiert.
- Bei Erhärtung des Verdachts auf strafbare Handlungen darf der Systembetreiber beweissichernde Massnahmen wie z.B. Keystroke Logging oder Netzwerk-Sniffer einzusetzen.
- Der Systembetreiber ist zur Vertraulichkeit verpflichtet.
- Der Systembetreiber gibt die Ansprechpartner für die Betreuung seiner Benutzer bekannt.
- Der Systembetreiber ist verpflichtet, im Verkehr mit Rechnern und Netzen anderer Betreiber deren Benutzungs- und Zugriffsrichtlinien einzuhalten.
- Der Systembetreiber darf Internetseiten sperren.
- Der Systembetreiber ist berechtigt, Benutzern alle Kosten zu berechnen, die durch unzutreffende Störmeldungen oder einer nicht ordnungsgemässen oder unsachgemässen Nutzung der installierten Einrichtungen entstanden sind.

Haftung des Systembetreibers - Haftungsausschluss

Der Systembetreiber übernimmt keine Garantie dafür, dass die Systemfunktionen den speziellen Anforderungen des Nutzers entsprechen oder dass das System fehlerfrei und ohne Unterbrechung läuft.

Der Systembetreiber kann nicht die Unversehrtheit (bzgl. Zerstörung, Manipulation) und Vertraulichkeit der bei ihm gespeicherten Daten garantieren.
Der Systembetreiber haftet nicht für Schäden gleich welcher Art, die dem Benutzer aus der Inanspruchnahme der ICT-Ressourcen entstehen; ausgenommen ist vorsätzliches Verhalten des Systembetreibers oder der Personen, deren er sich zur Erfüllung seiner Aufgaben bedient.

Folgen einer missbräuchlichen oder gesetzeswidrigen Benutzung

Bei Verstössen gegen gesetzliche Vorschriften oder gegen die Bestimmungen dieser Benutzungsrichtlinien kann der Systembetreiber die Benutzungsberechtigung einschränken oder ganz beziehungsweise teilweise entziehen. Es ist dabei unerheblich, ob der Verstoss einen Schaden zur Folge hatte oder nicht.
Bei schwerwiegenden oder wiederholten Verstössen kann ein Benutzer auf Dauer von der Benutzung sämtlicher ICT-Ressourcen ausgeschlossen werden.
Verstösse gegen gesetzliche Vorschriften oder gegen die Bestimmungen dieser Benutzungsrichtlinien werden auf ihre strafrechtliche Relevanz sowie auf zivilrechtliche Ansprüche hin überprüft. Der Systembetreiber behält sich die Verfolgung strafrechtlicher Schritte sowie zivilrechtlicher Ansprüche ausdrücklich vor.

Wartungsfenster

Unsere Wartungsfenster sind von 12:15 bis 12:45, von 17:15 bis 17:45 und ab 21:30 bis 07:00 Uhr. In diesen Zeiten können Systeme ohne Ankündigung für Benutzende nicht zur Verfügung stehen.

Sonstige Regelungen

Für die Nutzung von ICT-Ressourcen können in gesonderten Ordnungen Gebühren festgelegt werden.
Für bestimmte Systeme können bei Bedarf ergänzende oder abweichende Nutzungsregelungen festgelegt werden.
Der Systembetreiber kann diese IT Nutzungsrichtlinien jederzeit einseitig ändern. Diese treten mit der Kommunikation per E-Mail an alle registrierten Nutzer unmittelbar in Kraft und werden mit der weiteren Nutzung der ICT Ressourcen akzeptiert.
Gerichtsstand für alle aus dem Benutzungsverhältnis erwachsenden rechtlichen Ansprüche ist Zürich.

WLAN Nutzungsbedingungen

Nutzungsbedingungen

Sie sind im Begriff auf das Internet zuzugreifen über einen drahtlosen Netzwerkdienst des Zürcher Lehrbetriebsverband ICT ("ZLI"). Die Benutzung dieses Dienstes ist über die hier vorliegenden Nutzungsbedingungen ("die Vereinbarung") des WLAN-Internetzugangs geregelt. Sie dürfen diesen Dienst nur benutzen, wenn Sie sich ausdrücklich mit den Nutzungsbedingungen dieser Vereinbarung einverstanden erklären. Bitte lesen Sie diese Vereinbarung sorgfältig durch bevor Sie auf den Dienst zugreifen. Durch die Benutzung des WLAN akzeptieren Sie die Bedingungen der Vereinbarung. Die Bedingungen der Vereinbarung regeln und betreffen nur die Benutzung des WLAN-Internetzugangs und betreffen in keiner Weise andere Beziehungen zwischen Ihnen und dem ZLI.

Zugriff und Verfügbarkeit

Dieser Dienst darf ausschliesslich von Mitarbeitenden, Kursteilnehmenden, Kursleitenden oder anerkannten Gästen des ZLI genutzt werden. Anerkannte Gäste sind solche, denen offiziell einen gültigen Benutzernamen mit Passwort für die Nutzung dieses Dienstes von einem autorisierten Mitarbeitenden zugeteilt wurde. Unerlaubte Nutzung dieses Dienstes ist grundsätzlich untersagt. Personen denen kein gültiger Benutzername mit Passwort für die Nutzung dieses Dienstes zugeteilt wurde, sollten alle weiteren Versuche zur Nutzung dieses Dienstes unterlassen. Benutzername und Passwort dürfen nur durch die Person verwendet werden, der sie ursprünglich zugeteilt wurden. Benutzer sind für sämtliche Tätigkeiten haftbar die mit ihrem zugeteilten Benutzernamen und Passwort durchgeführt werden. Benutzer dürfen Ihren Benutzer-namen und Passwort keinesfalls anderen Personen oder Gruppen zur Nutzung des Dienstes weitergeben. Der Dienst ist nur in den Schulräumlichkeiten verfügbar. Die Abdeckung, Geschwindigkeit und Qualität des Dienstes können variieren. Der Dienst kann z.B. durch Notfälle, Übertragungsgeräte, Netzwerkprobleme, Beschränkungen, Interferenzen, schwachen Signalpegeln oder Unterhaltsarbeiten nicht verfügbar sein. Der WLAN-Internetzugang bietet keinen unbeschränkten Internetzugang und ist nur für definierte Dienste für Gäste des ZLI gedacht. Zugriff auf den Dienst geschieht allein nach dem Ermessen des ZLI und Ihr Zugriff auf den Dienst kann jederzeit blockiert, eingestellt oder beendet werden. Der ZLI kann nicht für Beschädigungen, Verluste, Kosten oder Aufwände verantwortlich gemacht werden, die durch die Nutzung oder Beendigung des Dienstes oder als Folge davon entstehen.

Nutzung des Dienstes

Benutzer des Dienstes erklären sich einverstanden mit den Verhaltensregeln und Sicherheitsbestimmungen des ZLI und nutzen den Dienst nicht für Zwecke die ungesetzlich sind oder durch diese Vereinbarung untersagt wurden. Die folgende, nicht abschliessende Aufzählung beinhaltet untersagte Verwendungszwecke:

- Nutzung des Dienstes in einer Art und Weise, die Urheberrechte, Patente, Markenrechte oder geistiges Eigentum anderer verletzt
- Nutzung des Dienstes in einer Art und Weise, die den Betrieb des Dienstes erheblich beeinträchtigt
- Nutzung des Dienstes zur Verleumdung, Diffamierung, Belästigung, vorsätzlicher Falschdarstellung, Betrug oder Veröffentlichung vertraulicher Informationen
- Verbreitung von Viren, Trojanern, Würmern oder anderen Computerprogrammen zur Beschädigung, Behinderung, heimlichem Abfangen, Enteignung von Systemen, Daten oder persönlichen Informationen
- Nutzung des Dienstes um illegal oder unautorisiert Zugang zu anderen Computern oder Netzwerken zu erhalten
- Nutzung des Dienstes um Daten Dritter ohne deren Wissen und Einwilligung abzufangen, zu sammeln oder zu speichern
- Versenden unerwünschter Mitteilungen, "Spam" oder "Junk Mail"
- Erweitern des Dienstes um den Dienst via Proxy oder anderer Mittel an andere Computer/Benutzer anzubieten

Der ZLI behält sich das Recht vor, die Nutzung des Dienstes zu überwachen damit die Einhaltung dieser Vereinbarung oder anwendbarer Gesetze überprüft werden kann. Der ZLI behält sich das Recht vor die Übertragung zu überwachen um persönlich identifizierbare Informationen für die Konfiguration des Dienstes zu sammeln, die Verfügbarkeit und das Verhalten des Dienstes zu überwachen und Probleme im Zusammenhang mit dem Dienst zu beheben.

Haftungsbeschränkung

Benutzer des ZLI WLAN-Internetzugang nutzen den Dienst auf eigene Gefahr. Der ZLI kann nicht verantwortlich gemacht werden für Schäden die durch die Nutzung des Dienstes entstehen. Die folgende, nicht abschliessende Aufzählung beinhaltet mögliche Schäden:

- Verlust vertraulicher Daten oder Beeinträchtigung der Sicherheit
- Personen oder Sachschaden
- Beschädigungen durch Unterbruch oder Ausfall des Dienstes oder Datenverlust
- Verlust durch unautorisierten Zugriff durch Viren oder anderen schädlichen Komponenten
- Unterbruch durch Datenverlust oder die Übertragung
- Verluste durch Waren oder Dienste die über den Dienst gekauft worden sind, durch Meldungen oder Daten die über den Dienst empfangen wurden oder durch Transaktionen die über den Dienst getätigt wurden

ZÜRCHER LEHRBETRIEBSVERBAND ICT

Datenschutz und Sicherheit

Die Benutzer werden darauf hingewiesen, dass die durch diesen Dienst bereitgestellte drahtlose Internetverbindung nicht sicher ist. Verbindungen können durch Fremde abgefangen werden. Der Benutzer ist verantwortlich zusätzliche, notwendig erscheinende technische Werkzeuge zum Schutz sensibler Daten zu installieren und anzuwenden. Der Benutzer ist verantwortlich für die Sicherheit seines Computers oder vernetzter Geräte für die er die Verantwortung trägt. Der ZLI empfiehlt die Installation einer Anti-Malware Software und einer persönlichen Firewall um das Gerät vor unbefugtem Zugriff und Beschädigung zu schützen.