

# **Nutzungsordnung für die EDV-Infrastruktur am Zentralinstitut für Kunstgeschichte**

Das Zentralinstitut für Kunstgeschichte München (nachstehend ZI) betreibt eine EDV-Infrastruktur und bietet für Mitarbeiter, Stipendiaten, Gastwissenschaftler und Praktikanten Rechnerdienste und Rechnerdienstleistungen an. Sie nutzt dabei die vom Leibniz-Rechenzentrum der Bayerischen Akademie der Wissenschaften (LRZ) betriebene Netzwerk-Infrastruktur.

## Die Nutzungsordnung

- orientiert sich an den Benutzungsrichtlinien für Informationsverarbeitungssysteme des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften (LRZ),
- regelt Aufgaben, Rechte und Pflichten der IT-Betreuung,
- stellt Grundregeln für einen ordnungsgemäßen Betrieb der EDV-Infrastruktur des ZI auf,
- weist hin auf die zu wahren Rechte Dritter (z.B. bei Softwarelizenzen, Auflagen der Netzbetreiber, Datenschutzaspekte),
- verpflichtet die Nutzer zu korrektem Verhalten und zum ökonomischen Gebrauch der angebotenen Ressourcen,
- klärt auf über eventuelle Maßnahmen des Betreibers bei Verstößen gegen die Benutzungsrichtlinien.

## **1. Geltungsbereich**

Diese Nutzungsordnung gilt für die Nutzung der EDV-Infrastruktur des ZI. Zur EDV-Infrastruktur zählen insbesondere Datenverarbeitungsanlagen, Kommunikationssysteme und sonstige Einrichtungen zur rechnergestützten Datenverarbeitung, nebst der dazugehörigen Software.

## **2. Aufgaben der IT-Betreuung**

- (1) Die IT-Betreuung des ZI hat insbesondere folgende Aufgaben:
  1. Planung, Realisierung und Betrieb der Datenverarbeitungsanlagen
  2. Koordinierung der Beschaffung von Datenverarbeitungsanlagen
  3. Erwerb, Verwaltung, Dokumentation und Pflege von Standardsoftware
  4. Anwenderunterstützung
- (2) Die IT-Betreuung ist überdies für die Planung, Installation und den Betrieb rechnergestützter Informations- und Kommunikationsnetze einschließlich der erforderlichen Netze, zentralen Server sowie der Datenkommunikationssysteme zuständig.  
Diesbezüglich obliegen der IT-Betreuung insbesondere folgende Aufgaben:
  1. Bereitstellung und Aufrechterhaltung eines störungsfreien und möglichst ununterbrochenen Betriebes des Kommunikationsnetzes
  2. Koordination des Ausbaus und der Wartung des Kommunikationsnetzes
  3. Verwaltung der Adress- und Namensräume
  4. Bereitstellung von Netzwerkdiensten und zentraler Netzwerk-Server (z.B. Mail-, WWW-, Fileserver)
  5. Unterstützung der Mitarbeiter bei der Anwendung der Dienste
  6. Realisierung von Sicherheitsmaßnahmen (wie z.B. Schutz vor schadensverursachender Software wie Viren, Anti-Relay und Anti-SPAM Maßnahmen bei E-Mail, Firewall, Verschlüsselung sensibler Daten)
- (3) Die IT-Betreuung trifft die erforderlichen technischen und organisatorischen Maßnahmen, damit nur Personen mit gültiger Nutzungsberechtigung die EDV-Infrastruktur nutzen können. Soweit technisch möglich hat die IT-Betreuung sicherzustellen, dass die

Nutzung der EDV-Infrastruktur nach Ablauf einer zeitlich befristeten Nutzungsberechtigung nicht mehr möglich ist.

### **3. Rechte und Pflichten der IT-Betreuung**

- (1) Die IT-Betreuung des ZI führt über die erteilten Nutzungsberechtigungen eine Datei, in der die zugelassenen Nutzer aufgeführt werden.
- (2) Die IT-Betreuung ist berechtigt, nach Ablauf der Nutzungsberechtigung alle Daten und Programme des Nutzers zu sperren und zu löschen.
- (3) Eingehende E-Mail kann nach Ende der Nutzungsberechtigung an eine vom Nutzer schriftlich zu benennende E-Mail-Adresse weitergeleitet werden (befristet für die Dauer von 3 Monaten bei Mitarbeitern und 6 Wochen bei Hilfskräften und Stipendiaten). Benennt der Nutzer keine Adresse oder ist die Frist abgelaufen, wird eingehende E-Mail abgewiesen.
- (4) Soweit dies zur Störungsbeseitigung, zur Systemadministration und -erweiterung oder aus Gründen der Systemsicherheit sowie zum Schutz der Nutzerdaten erforderlich ist, kann die IT-Betreuung die Nutzung ihrer Ressourcen vorübergehend einschränken oder einzelne Nutzerkennungen vorübergehend sperren. Sofern möglich, sind die betroffenen Nutzer hierüber im Voraus zu unterrichten.
- (5) Sofern tatsächliche Anhaltspunkte dafür vorliegen, dass sich ein Nutzer über die EDV-Infrastruktur rechtswidrigen Datenzugang verschafft oder dass ein Nutzer auf den Servern der IT-Betreuung rechtswidrige Inhalte zur Nutzung bereithält, kann die IT-Betreuung die weitere Nutzung verhindern, bis die Rechtslage hinreichend geklärt ist.
- (6) Die IT-Betreuung ist nach Maßgabe der nachfolgenden Regelungen berechtigt, die Inanspruchnahme der Datenverarbeitungssysteme durch die einzelnen Nutzer zu dokumentieren und auszuwerten, jedoch nur soweit dies erforderlich ist:
  1. zur Gewährleistung eines ordnungsgemäßen Systembetriebs oder
  2. zur Ressourcenplanung und Systemadministration oder
  3. zum Schutz der personenbezogenen Daten anderer Nutzer oder
  4. zu Abrechnungszwecken oder
  5. für das Erkennen und Beseitigen von Störungen oder
  6. zur Aufklärung und Unterbindung rechtswidriger, insbesondere strafbarer Nutzung.
- (7) Die IT-Betreuung ist auch berechtigt, unter Beachtung des Datengeheimnisses Einsicht in die Benutzerdateien zu nehmen, soweit dies erforderlich ist zur Beseitigung aktueller Störungen oder zur Aufklärung und Unterbindung von Missbräuchen. Eine Einsichtnahme in die Nachrichten- und E-Mail-Postfächer ist jedoch nur zulässig, soweit dies zur Behebung aktueller Störungen im Nachrichtendienst unerlässlich ist. In jedem Fall ist die Einsichtnahme zu dokumentieren, und der betroffene Benutzer ist nach Zweckerreichung unverzüglich zu benachrichtigen.
- (8) Die Verbindungs- und Nutzungsdaten im Nachrichtenverkehr (insbes. Mail-Nutzung) können dokumentiert werden. Es dürfen jedoch nur die näheren Umstände der Telekommunikation – nicht aber die nicht-öffentlichen Kommunikationsinhalte – erhoben, verarbeitet und genutzt werden. Die Verbindungs- und Nutzungsdaten der Online-Aktivitäten im Internet und sonstigen Diensten, die die IT-Betreuung zur Nutzung bereithält oder zu denen die IT-Betreuung den Zugang zur Nutzung vermittelt, sind frühestmöglich, spätestens unmittelbar am Ende der jeweiligen Nutzung zu löschen, soweit es sich nicht um Abrechnungsdaten handelt.
- (9) Nach Maßgabe der gesetzlichen Bestimmungen ist die IT-Betreuung zur Wahrung des Fernmelde- und Datengeheimnisses verpflichtet.

### **4. Rechte und Pflichten der Nutzer**

- (1) Der Nutzer ist verpflichtet, darauf zu achten, dass er die vorhandenen Betriebsmittel (Arbeitsplätze, CPU-Kapazität, Plattspeicherplatz, Leitungskapazitäten,

Peripheriegeräte und Verbrauchsmaterial) verantwortungsvoll und ökonomisch sinnvoll nutzt. Der Nutzer ist verpflichtet, Beeinträchtigungen des Betriebes, soweit sie vorhersehbar sind, zu unterlassen und nach bestem Wissen alles zu vermeiden, was Schaden an der EDV-Infrastruktur oder bei anderen Nutzern verursachen kann. Alle Datenverarbeitungsanlagen, Informations- und Kommunikationssysteme und sonstigen Einrichtungen der IT-Betreuung sind sorgfältig und schonend zu behandeln.

- (2) Ohne ausdrückliche Einwilligung der IT-Betreuung sind keine Eingriffe in die Hardwareinstallation der IT-Betreuung vorzunehmen und die Konfiguration der Betriebssysteme, der Systemdateien, der systemrelevanten Nutzerdateien und des Netzwerks nicht zu verändern. Dem Nutzer ist es ohne ausdrückliche Einwilligung der IT-Betreuung nicht gestattet, Hardware oder Software zu installieren. Ein Anspruch auf Installation und Nutzung von anderer als der installierten Hard- oder Software besteht nicht. Störungen, Beschädigungen und Fehler an EDV-Einrichtungen und Datenträgern der IT-Betreuung sind nicht selbst zu beheben, sondern unverzüglich den Mitarbeitern der IT-Betreuung zu melden.
- (3) Der Nutzer ist verpflichtet, fremde Benutzerkennungen und Passwörter weder zu ermitteln noch zu nutzen, keinen unberechtigten Zugriff auf Informationen anderer Nutzer zu nehmen und bekannt gewordene Informationen anderer Nutzer nicht ohne Genehmigung weiterzugeben, selbst zu nutzen oder zu verändern.
- (4) Der Nutzer ist verpflichtet, Vorkehrungen zu treffen, damit unberechtigten Dritten der Zugang zur EDV-Infrastruktur des ZI verwehrt wird; dazu gehört es insbesondere, primitive, naheliegende Passwörter nicht zu verwenden und sich am Ende der Benutzung ordnungsgemäß per Logout abzumelden. Der Nutzer 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.
- (5) Der Benutzer ist des Weiteren verpflichtet,
  1. bei der Benutzung von Software (Quellen, Objekte), Dokumentationen und anderen Daten die gesetzlichen Regelungen (Urheberrechtsschutz, Copyright) einzuhalten;
  2. 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;
  3. 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;
  4. der Leitung der IT-Betreuung auf Verlangen in begründeten Einzelfällen – insbes. bei begründetem Missbrauchsverdacht und zur Störungsbeseitigung – zu Kontrollzwecken Auskünfte über Programme und benutzte Methoden zu erteilen sowie Einsicht in die Programme zu gewähren;
  5. eine Verarbeitung personenbezogener Daten mit der IT-Betreuung abzustimmen und – unbeschadet der eigenen datenschutzrechtlichen Verpflichtungen des Nutzers – die von der IT-Betreuung vorgeschlagenen Datenschutz- und Datensicherheitsvorkehrungen zu berücksichtigen;
- (6) Jedes rechtswidrige oder nach allgemeingültigen ethischen Maßstäben unangemessene Nutzungsverhalten ist zu unterlassen. Auf die folgenden Straftatbestände wird besonders hingewiesen:
  1. Ausforschen fremder Passworte, Ausspähen und Abfangen von Daten (§202 a|b|c StGB)
  2. unbefugtes Verändern, Löschen, Unterdrücken oder Unbrauchbarmachen von Daten (§303 a StGB)
  3. Computersabotage (§303 b StGB) und Computerbetrug (§263 a StGB)

4. die Verbreitung von Propagandamitteln verfassungswidriger Organisationen (§86 StGB) oder Gewaltdarstellung (§131 StGB)
  5. die Verbreitung von Pornographie im Netz (§§184ff. StGB), insbesondere Abruf oder Besitz von Dokumenten mit Kinderpornographie (§184 Abs.1 Ziff. 5 StGB)
  6. Ehrdelikte wie Beleidigung oder Verleumdung (§§ 185 ff. StGB)
  7. Urheberrechtsverletzungen, z.B. durch rechtswidrige Vervielfältigung von Software bzw. Anbieten eines Films oder Musikstückes in einer Filesharingbörsen (§§ 106 ff. UrhG)
- (7) Der Nutzer ist verpflichtet rechtzeitig vor Beendigung seiner Nutzungsberechtigung, dem ZI alle Daten, Programme und Dokumentationen, die ihm vom ZI überlassen wurden oder auf die das ZI einen sonstigen vertraglichen oder gesetzlichen Anspruch hat, in geeigneter Form zu übergeben. Soweit nichts anderweitiges ausdrücklich vereinbart wurde, ist es dem Nutzer nicht gestattet, Kopien von Daten, Programmen und Dokumentationen nach Beendigung der Nutzungsgenehmigung zurückzubehalten.
- (8) Privatnutzung des WWW-Dienstes:
1. Die Privatnutzung ist nur zulässig, soweit diese in geringfügigem Umfang erfolgt und die Sicherheit der IT-Systeme nicht gefährdet. Hiervon umfasst ist auch die Speicherung privater Daten und Downloads. Dienstliche Belange haben stets Vorrang und dürfen durch die Privatnutzung nicht beeinträchtigt werden.
  2. Die Privatnutzung darf nicht zur Verfolgung gewerblicher oder geschäftsmäßiger Interessen erfolgen. Die Privatnutzung für die Besorgung von Rechtsgeschäften des täglichen Lebens (z.B. Kauf von Fahrkarten) ist zulässig.
  3. Die Privatnutzung darf nicht zu Zwecken erfolgen, die die Interessen oder das Ansehen des ZI in der Öffentlichkeit beeinträchtigen können. Insbesondere haben der Abruf kostenpflichtiger Internetseiten, das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenzi- und urheberrechtliche oder strafrechtliche Bestimmungen verstößen, das Abrufen, Verbreiten oder Speichern von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen sowie Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z.B. Angriffe auf externe Webserver) zu unterbleiben.
  4. Die Gestattung der Privatnutzung stellt eine freiwillige Leistung des Dienstherrn dar. Aus der Gestattung der Privatnutzung kann kein Rechtsanspruch der Beschäftigten hergeleitet werden. Es besteht auch kein Rechtsanspruch auf den Zugriff gefilterter Internetinhalte. Die Gestattung der Privatnutzung kann jederzeit durch einseitige Erklärung widerrufen werden. Eine Haftung für das Funktionieren des WWW-Dienstes ist ausgeschlossen.
- (9) Nutzung des E-Mail-Dienstes:
1. Die Beschäftigten erhalten zu dienstlichen Zwecken Zugang zum E-Mail-Dienst (Zuweisung einer dienstlichen E-Mail-Adresse sowie eines personenbezogenen Postfaches). Für die Inhalte und die Pflege des personenbezogenen Postfaches ist der jeweilige Beschäftigte persönlich verantwortlich.
  2. Die Postfächer sind von den betroffenen Beschäftigten zu pflegen. Die Pflege
  3. beinhaltet die regelmäßige Überprüfung des Posteinganges. Bei vorhersehbarer längerer Abwesenheit (Urlaub, Dienstreise) sollte der Abwesenheitsassistent aktiviert werden (Weiterleitungsfunktion und/oder Abwesenheitsmitteilung).
  4. Die Beschäftigten sind bei der Nutzung des E-Mail-Dienstes zu besonderer Sorgfalt verpflichtet. Anhänge von E-Mails sollen nur bei Verlässlichkeit der Quellen geöffnet werden. Meldet die Virenerkennung einen Virus, ist unverzüglich, ohne weitere Aktivitäten am Computer vorzunehmen, die IT-Betreuung zu informieren. Diesbezügliche und sonstige Hinweise der IT-Betreuung sind zu beachten.

5. Für die Nutzung des dienstlich bereitgestellten E-Mail-Dienstes zu privaten Zwecken (Privatnutzung) gelten die unter (8) aufgeführten Bestimmungen des WWW-Dienstes.
6. Bei der Privatnutzung der dienstlichen E-Mail-Adresse ist besonders darauf zu achten und sicherzustellen, dass die Interessen oder das Ansehen des ZI nicht beeinträchtigt werden. Virenverseuchte E-Mails und unerwünschte Werbung (Spam) werden wie dienstliche E-Mails behandelt und gegebenenfalls gelöscht.

## **5. Haftung des Nutzers**

- (1) Der Benutzer haftet für alle Nachteile, die dem ZI durch missbräuchliche oder rechtswidrige Verwendung der EDV-Infrastruktur oder dadurch entstehen, dass der Nutzer seinen Pflichten aus den Benutzungsrichtlinien nicht nachkommt.
- (2) Der Nutzer haftet auch für Schäden, die durch eine unbefugte Nutzung durch Dritte entstehen, wenn er diese Drittnutzung, z.B. durch Weitergabe der Benutzerkennung, zu vertreten hat.
- (3) Der Nutzer hat das ZI, soweit er dafür haftbar gemacht werden kann, von allen Ansprüchen freizustellen, wenn Dritte das ZI wegen eines missbräuchlichen oder rechtswidrigen Verhaltens des Nutzers auf Schadenersatz, Unterlassung oder in sonstiger Weise in Anspruch nehmen. Das ZI wird dem Nutzer den Streit verkünden, sofern Dritte gegen das ZI gerichtlich vorgehen.

Ergänzend zu diesen Regelungen gelten in ihrer jeweils gültigen Fassung

- die Benutzungsrichtlinien für Informationsverarbeitungssysteme und die Betriebsregelungen des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften (LRZ), einsehbar unter <http://www.lrz.de/wir/regelwerk/benutzungsrichtlinien.pdf>
- sowie die Richtlinien zum Betrieb des Münchener Wissenschaftsnetzes (MWN), einsehbar unter [https://www.lrz.de/wir/regelwerk/richtlinien\\_mwn/](https://www.lrz.de/wir/regelwerk/richtlinien_mwn/)

München, 13.05.2019

Ulrich Pfisterer

Direktor