Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Behrendt, Andrea (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8M9__
  - Rechnernummer: _NRW2NL1350
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Benner-Jungbluth, Miranda (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8EN__
  - Rechnernummer: _NRW2NL1351
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Diedenhofen, Charlotte (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8EL__
  - Rechnernummer: _NRW2NL1352
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Thoennes, Maria (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8J5__
  - Rechnernummer: _NRW2NL1353
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Nettersheim, Andreas (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8GZ__
  - Rechnernummer: _NRW2NL1354
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Gercek, Silke (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8F2__
  - Rechnernummer: _NRW2NL1355
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Byvank, Daniela (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8GQ__
  - Rechnernummer: _NRW2NL1356
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Kuchenwald, Monika (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8J2__
  - Rechnernummer: _NRW2NL1357
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Kosche, Martina (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8F9__
  - Rechnernummer: _NRW2NL1358
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Labusch, Alexandra (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8FG__
  - Rechnernummer: _NRW2NL1359
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Lambergar, Sabine (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8D2__
  - Rechnernummer: _NRW2NL1360
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Langner, Markus (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8EF__
  - Rechnernummer: _NRW2NL1361
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Gressard, Isabell (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8J0__
  - Rechnernummer: _NRW2NL1362
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Fahrenbruch, Paula (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8DA__
  - Rechnernummer: _NRW2NL1363
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Rutsch, Christina (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8E9__
  - Rechnernummer: _NRW2NL1364
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Seeck, Oliver (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8EE__
  - Rechnernummer: _NRW2NL1365
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Mueller, Juergen (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8DP__
  - Rechnernummer: _NRW2NL1366
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Weiser, Christiane (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8DG__
  - Rechnernummer: _NRW2NL1367
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Pasalk, Sarah (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8G5__
  - Rechnernummer: _NRW2NL1368
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift

Nutzungsregelung - dienstliche Endgeräte für die ausbildungsfachliche Arbeit der Seminarausbilderinnen und Seminarausbilder an den ZfsL

1. Geltungsbereich

Die Nutzungsregelung gilt für die Nutzung der vom Land Nordrhein-Westfalen zur Verfügung gestellten dienstlichen Endgeräte für Seminarausbilderinnen und Seminarausbilder aller Lehrämter an den Zentren für schulpraktische Lehrerausbildung.

2. Ausstattung

Das Land Nordrhein-Westfalen stellt jeweils die folgende Ausstattung zur Verfügung:

- ein mobiles Endgerät
- inkl. Maus und Tragetasche
- einen verschlüsselten USB-Stick
- bei nachgewiesener Schwerbehinderung eine entsprechend barrierefreie Ausstattung

Die Ausstattung bleibt auch nach Überlassung Eigentum des Landes Nordrhein-Westfalen.

3. Einsatzbereich

Die Ausstattung steht den genannten Personen

- ausschließlich zur dienstlichen Nutzung im Rahmen ihrer Tätigkeit als Seminarausbilderin bzw. Seminarausbilder,
- räumlich innerhalb wie auch außerhalb der ZfsL,
- zeitlich bis auf Widerruf,
- unentgeltlich,

zur Verfügung.

4. Nutzungsbedingungen

4.1 Beachtung geltender Rechtsvorschriften

Die gesamte Rechtsordnung, insbes. die Bestimmungen des Urheber-, Jugendschutz-, Datenschutz- und Strafrechts, bildet bei der Nutzung der Ausstattung den gesetzlichen Rahmen.

Insbesondere ist es verboten, pornographische, gewaltdarstellende oder -verherrlichende, rassistische, menschenverachtende oder denunzierende Inhalte über die Ausstattung zu verarbeiten, es sei denn, ausbildungsfachliche Gründe legitimieren eine solche Verarbeitung.

Bei der Verwendung urheberrechtlich geschützten Materials oder Softwareanwendungen sind deren Lizenzbedingungen zu beachten. Ohne Besitz der entsprechenden Nutzungsrechte ist eine Verarbeitung geschützter Materialien sowie die Nutzung von Softwareanwendungen untersagt.

Bei der Verarbeitung personenbezogener Daten sind die Vorgaben der EU-Datenschutzgrundverordnung (DSGVO), des Datenschutzgesetzes NRW (DSG NRW), des Schulgesetzes NRW (SchulG NRW) und der Verordnungen über die zur Verarbeitung zugelassenen Daten (VO-DV I, VO-DV II) zu beachten.

4.2 Zugriff auf die Ausstattung

Die Ausstattung darf nicht an Dritte weitergegeben oder diesen zum Gebrauch überlassen werden. Diese Einschränkung umfasst nicht die Mitnutzung der Ausstattung durch beteiligte Personen im Kontext ausbildungsfachlicher Szenarien (z. B. Seminare, Ausbildungsunterricht). Dabei ist dann sicher zu stellen, dass diese Personen keinen Zugriff auf personenbezogene Daten haben, die ggf. auf diesem Gerät gespeichert sind.

Im öffentlichen Raum ist die mobile Ausstattung nicht unbeaufsichtigt zu lassen.

4.3 Zugang zur Ausstattung

In der Grundkonfiguration sind auf den Notebooks drei Nutzeraccounts eingerichtet:

- individueller Standard-Account
  - Dieser Account ist für die ausbildungsfachliche Arbeit vorgesehen.
    Der Account besitzt nur die für diese Tätigkeiten erforderlichen Berechtigungen.
- individueller Admin-Account
  - Dieser Account ist mit weitgehenden Berechtigungen ausgestattet und dient zur Installation von Software oder der Anpassung von Einstellungen durch die betreffende Person.
    Der Account darf nur zu diesem Zweck verwendet werden und ist nicht für die ausbildungsfachliche Arbeit zu nutzen.
- Standard-Admin-Account
  - Dieser Account dient nur der Administration des Gerätes durch den Informationstechnischen Dienst des ZfsL (ITD-ZfsL) und ist für die Nutzer nicht zugänglich.

Die Zugänge zu den Accounts sind mit initialen Passwörtern gesichert, welche bei der Erstanmeldung zu ändern sind. Die Passwörter sind sicher aufzubewahren und Dritten nicht zur Kenntnis zu geben. Sollte der Verdacht bestehen, dass ein Passwort Dritten bekannt geworden sein sollte, ist dieses unverzüglich zu ändern.

Das Passwort muss mindestens acht Zeichen lang sein, Groß- und Kleinbuchstaben sowie mindestens eine Ziffer und ein Sonderzeichen (z.B.: +, -, *, #, ?, !) beinhalten.

Das Gerät ist bei jedem (auch kurzem) Verlassen des Arbeitsplatzes zu sperren.

4.4 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Malware vorkonfiguriert:

- Nutzeraccounts mit unterschiedlichen Berechtigungen und initialen Nutzerpasswörtern
- automatische Gerätesperre nach 15 Minuten der Inaktivität

- aktivierte Schutzsoftware (Windows-Defender: Desktop-Firewall und Antiviren-Schutz)
- aktivierte automatische Malware-Prüfung von angeschlossenen Speichermedien (z. B. USB-Sticks)
- aktivierte automatische Updates des Betriebssystems und ggf. der vorinstallierten Software

Den Nutzerinnen und Nutzern der Notebooks ist es untersagt, die vorkonfigurierten Maßnahmen zu deaktivieren.

Darüber hinaus ist es untersagt

- den individuellen Standardaccount mit Administrationsrechten auszustatten,
- den individuellen Administratorenaccount für die alltägliche Arbeit zu verwenden,
- den Administratorenaccount des ITD-ZfsL zu verändern oder zu löschen,
- weitere Accounts mit Administratorberechtigungen anzulegen,
- die voreingestellten Standard-Berechtigungsrichtlinien („Gruppenrichtlinien“) des Betriebssystems zu verändern,
- die automatische Gerätesperre zu deaktivieren,
- den Passwortschutz zu deaktivieren,
- für den Standard-Account und den Admin-Account das gleiche Passwort zu verwenden,
- Nutzerpasswörter weiterzugeben,
- Nutzerpasswörter unverschlüsselt auf dem Rechner abzuspeichern oder am Endgerät anzubringen,
- Änderungen an der Einstellung der Firewall vorzunehmen,
- den Virenschutz zu deaktivieren.

Warnhinweise der Antiviren-Software und der Desktop-Firewall sind zu beachten und Sicherheitsvorfälle dem ITD-ZfsL anzuzeigen.

4.5 Softwareinstallation

Die genannten Benutzergruppen dürfen über den individuellen Admin-Account eigenständig Softwareanwendungen auf dem Endgerät installieren und diese verwenden. Dabei sind die Lizenzbedingungen sowie Vorgaben zur Verarbeitung personenbezogener Daten zu beachten (siehe 4.1). Die *Leitlinie für die rechtskonforme Nutzung individueller Software* unterstützt die Benutzer bei der Auswahl von Software.

Eigenständig installierte Software ist über Sicherheitsupdates auf dem aktuellen Stand zu halten.
Bei Fragen zum Datenschutz können sich die oben gennannten Personen an den zust. beh. Datenschutzbeauftragten des ZfsL wenden.

4.6 Weitere Sicherheitsmaßnahmen

Die Nutzerin oder der Nutzer hat für folgende Sicherheitsmaßnahmen eigenständig Sorge zu tragen:

- Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das Endgerät regelmäßig, in der Regel einmal pro Woche, mit dem

Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind zu bestätigen.

- Die Sicherung der individuell von der Nutzerin oder dem Nutzer vorgenommener Einstellungen, die Installation individueller Programme und Anwendungen wie auch die monatliche Erstellung von Backups der Daten und Dokumenten obliegt in der eigenen Verantwortung. Für die regelmäßige Datensicherung ist ausschließlich der verschlüsselte USB-Stick oder andere vom ZfsL zugelassene Speicher zu verwenden
- Alle Netzwerke sind im Verbindungsdialog des Betriebssystems zwingend als „öffentliche Netzwerke“ einzuordnen.
- Der Zugang zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk des ZfsL, das eigene WLAN im häuslichen Arbeitszimmer, einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zu verwendenden Netzwerke, ist von der Nutzung abzusehen.
- Ein sicheres Passwort zur Administrationsoberfläche des Routers, regelmäßige Sicherheitsupdates der Router-Firmware sowie WLAN-Verschlüsselung nach dem Stand der Technik (aktuell mindestens WPA2) des heimischen WLAN sind umzusetzen.

4.7 Cloudspeicher und Soziale Netzwerke

Die Ablage und der Austausch von Daten mit Personenbezug und Dokumenten, die solche Daten enthalten über Cloudspeicherdienste, zu denen seitens des Landes Nordrhein-Westfalens kein Dienstleistungsverhältnis besteht, ist untersagt. Gleiches gilt für die Verwendung von Diensten aus dem Bereich „Social Media“.

4.8 Technische Unterstützung

Die technische Unterstützung des durch den ITD-ZfsL umfasst

- die Grundkonfiguration der Endgeräte,
- eine Einweisung in die Grundkonfiguration der Endgeräte und Nutzung der Ausstattung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der Endgeräte,
- Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen.

4.9 Ansprüche, Schäden und Haftung

Die Ausstattung ist pfleglich zu behandeln. Störungen oder Schäden an der Ausstattung wie auch deren Verlust sind unverzüglich dem Informationstechnischen Dienst des ZfsL (ITD-ZfsL) anzuzeigen.

Kosten für die Beseitigung von Schäden, die vorsätzlich oder grob fahrlässig entstanden sind, werden der Nutzerin oder dem Nutzer in Rechnung gestellt (vgl. § 48 BeamtStG i.V.m. § 80 LBG und § 3 Abs. 7 TV-L).

5. Anerkennung der Nutzungsregelung

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsregelung vorzunehmen.

Giesen, Achim (ZfsL Koeln)

_____

Name, Vorname der Nutzerin oder des Nutzers

_____

Datum und Unterschrift

6. Übergabe der Ausstattung

Hiermit bestätige ich den Erhalt der folgenden Ausstattung:

- **Endgerät**
  - Bezeichnung: _Lenovo Thinkpad X13 Yoga_Gen1_____
  - Seriennummer: _R910E8E0__
  - Rechnernummer: _NRW2NL1369
- **Zubehör**
  - Netzteil
  - Maus
  - Tragetasche
- **USB-Stick**
- **Zugangsdaten**
  - Initial-Passwort individueller Standard-Account: **Leitung2020**
  - Initial-Passwort individueller Admin-Account: **Leitung-admin**

_____

Datum und Unterschrift