# Dienstanweisung für die Administratoren der IT-Systeme und IT-Dienste

# bei der Musterschule

(Stand 10/2013)

## 1 Geltungsbereich und Zweck der Dienstanweisung

Die Dienstanweisung regelt die Administration der informationstechnischen Systeme (IT-Systeme) und Dienste (IT-Dienste) im Hinblick auf die geltenden Bestimmungen des Datenschutzes und die gesetzlichen und betrieblichen Anforderungen an die Datensicherheit. Sie gilt für alle mit der Administration Beauftragten (Administratoren).

Ziel der Dienstanweisung ist der Schutz personenbezogener Daten und sonstiger gespeicherter Daten vor Missbrauch bei der elektronischen Datenverarbeitung.

## 2 Definitionen

Unter einem IT-System ist jegliches technische Gerät zu verstehen, welches als Einzelgerät oder als Ergänzung zu einem Einzelgerät zum Zwecke der elektronischen Datenverarbeitung genutzt wird. Eine umgangssprachliche Bezeichnung für solche IT-Systeme ist die Bezeichnung „Hardware“.

Datenverarbeitung ist das Erheben, Speichern, Verändern, Übermitteln, Sperren, Löschen und Nutzen von Daten, auch von personenbezogen Daten.

Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse von bestimmten oder bestimmbaren natürlichen Personen (Betroffene).

Unter einem IT-Dienst ist jede Anwendung zu verstehen, die zum Zwecke der elektronischen Datenverarbeitung erstellt worden ist.
Eine umgangssprachliche Bezeichnung für solche IT-Dienste ist die Bezeichnung „Software“.

## 3 Zuständigkeiten und Verantwortungsbereiche

### 3.1 Aufgaben des Administrators

Der Administrator hat dafür zu sorgen, dass die Benutzer von technischen Problemen entlastet werden und eine geordnete, einheitliche Weiterentwicklung des Nutzungskonzeptes erfolgt. Er hat folgende Aufgaben (bitte an die Gegebenheiten vor Ort anpassen!):

- □ das Netzwerk und seine Komponenten zu managen,
- □ die Nutzer bei der Bedarfsfeststellung zu beraten, den Geräte- und Sachmittelbedarf zu planen und ggf. Beschaffungsmaßnahmen einzuleiten,
- □ dafür zu sorgen, dass die Geräte installiert, die erforderlichen Softwaresysteme generiert und Benutzerprofile eingerichtet werden,
- □ dafür zu sorgen, dass neue Geräte und Produkte vor ihrem Einsatz zugelassen werden,
- □ Störungen einzugrenzen, nach Möglichkeit zu beheben,
- □ Maßnahmen für eine regelmäßige Datensicherung lt. Datensicherungskonzept durchzuführen,

- □ die Führung eines Hardware-/Software-Registers,
- □ die an den einzelnen Arbeitsplätzen installierten Gerätekonfigurationen und Softwareprodukte im Geräteverzeichnis zu aktualisieren,
- □ erforderliche Fortbildungsmaßnahmen für die Benutzer einzuleiten oder durchzuführen,
- □ Vorschläge für die Verbesserung und Weiterentwicklung des allgemeinen Einsatzkonzeptes zu machen und örtliche Regelungen für den Betrieb und die Instandhaltung der Ressourcen im Rahmen der allgemeinen Bestimmungen aufzustellen,
- □ die Beschaffung oder Erstellung von Betriebsunterlagen (Bedienungsanweisungen, Produktbeschreibungen),
- □ die Entwicklung, Dokumentation und Pflege von Verfahren, die Vorbereitung der formellen Freigabe von Verfahren in Abstimmung mit der fachlich zuständigen Stelle,
- □ die Erstellung von Unterlagen gemäß § 7 NDSG zur Vorabkontrolle von neuen/wesentlich geänderten automatischen Abrufverfahren sowie automatisierten Verfahren, in denen Daten im Sinne des § 3 NDSG verarbeitet werden ,
- □ die Zuarbeit bei der Erstellung und Aktualisierung von Verfahrensverzeichnissen von automatisierten, personenbezogenen Dateien für den Datenschutzbeauftragten der Schule,
- □ gegebenenfalls Auswertung der in den Programmen implementierten oder durch das jeweilige Betriebssystem vorgegebenen Protokollierungsmöglichkeiten, um Systemfehler, Fehlzugriffe oder Störungen zeitnah auswerten und beheben zu können,
- □ das Fortschreiben und Erweitern des Einsatzkonzepts.

Die Entscheidung über Grundsatzfragen und die Erteilung von Beschaffungs- oder Programmieraufträgen fällt der Schulträger in Abstimmung mit der Schulleitung.

### 3.2 Aufgaben des behördlichen Datenschutzbeauftragten

Der behördlich bestellte Datenschutzbeauftragte hat die Aufgabe, die Lehrkräfte in Datenschutzangelegenheiten zu beraten und die Einhaltung der Datenschutzvorschriften in der Schule zu überwachen. Er ist bei der Erfüllung seiner Aufgaben weisungsfrei. Die einzelnen Aufgaben des behördlichen Datenschutzbeauftragten ergeben sich aus § 8a NDSG.

### 3.3 Aufgaben der Schulleitung

Die Schulleitung ist verantwortlich für die Festlegung der Grundsätze der Informationsverarbeitung und die Freigabe von IT-Diensten.

## 4 Ausführungsbestimmungen

Für die Installation, Nutzung und Administration der von der Musterschule betriebenen IT-Systeme (Hardware) und IT-Dienste (Software) gelten folgende Bestimmungen:

### 4.1 Grundsätze

(1) Die Installation, Nutzung oder Administration der IT-Dienste ist ausschließlich zu dienstlichen Zwecken gestattet. Unzulässig ist jede Installation, Nutzung oder Administration, die geeignet ist, der Schule oder deren Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Gesetze und Verordnungen, insbesondere gegen datenschutzrechtliche, persönlichkeitsrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstößt.

(2) Die Installation und Nutzung nicht zugelassener IT-Dienste ist untersagt. IT-Dienste und Berechtigungen, die nicht mehr benötigt werden, sind zeitnah durch den Administrator zu deaktivieren. Falls ohne Beeinträchtigung für das Gesamtsystem möglich, sind die IT-Dienste zu deinstallieren oder zu löschen.

(3) Für die Durchführung dienstlicher Aufgaben dürfen nur zugelassene IT-Systeme und IT-Dienste verwendet werden. Der Anschluss privater Hardware an dienstliche IT-Systeme und die Nutzung privater Software ist nicht zulässig.
(4) IT-Dienste dürfen nicht ohne Genehmigung der Schulleitung installiert oder ausgeführt werden.
(5) Jede Weitergabe von Programmen und Daten an Dritte ist nur zulässig, wenn sie ausdrücklich gestattet ist.
(6) Die Übermittlung und Weitergabe von personenbezogenen Daten oder vertraulichen Informationen bedarf der Zustimmung des Informationseigentümers.

### 4.2 Entsorgung von IT-Systemen und Datenträgern

(1) Soll ein noch intakter Datenträger (hierzu gehören auch interne Datenspeicher aus Faxgeräten, Netzwerkdruckern und Kopiergeräten) mit vertraulichen Informationen verkauft, vermietet, ausgesondert, zurückgegeben oder einer neuen Nutzung zugeführt werden, ist zuvor der gesamte Datenträger von den Administratoren sicher zu löschen oder kontrolliert zu vernichten, so dass keine Rückschlüsse auf vorher gespeicherte Daten mehr möglich sind.
(2) Sofern keine sichere Entsorgung durchgeführt werden kann, ist ein externes Unternehmen zu beauftragen.

### 4.3 Informationstechnische Revision und Datenschutzkontrolle

Kontrollfunktionen im Rahmen der IT-Revision und der internen Datenschutzkontrolle dürfen nicht von den Administratoren wahrgenommen werden. Die Zuständigkeit für diese Aufgabe ist von der Schulleitung festzulegen.

### 4.4 Protokollierung und Kontrollen

Protokolldaten sind personenbezogen, da sie Aufschluss über die Aktivitäten eines Benutzers geben. Sie unterliegen nach dem Datenschutzrecht einer strikten Zweckbindung (§ 10 NDSG) und dürfen ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert, nicht jedoch für Zwecke der Verhaltens- oder Leistungskontrolle der Mitarbeiter verwendet oder ausgewertet werden. Grundsätzlich ist eine pauschale, flächendeckende und „vorbeugende“ Protokollierung aller Aktivitäten der Mitarbeiter an den IT-Systemen zur Verhaltens- und Leistungskontrolle nicht erforderlich und damit unzulässig.
*(Hinweis: Soweit die Nutzung der IT-Systeme zur Datenschutzkontrolle, der Datensicherung oder des ordnungsgemäßen Betriebes im System protokolliert wird, so sind mindestens Art und Umfang der Protokollierung, Zweckbindung, Zugriffsrechte, Auswertung und Löschungsfristen der Protokolldaten festzulegen. Die Durchführung von Kontrollen muss eindeutig geregelt werden. Auf mögliche in Betracht kommende Sanktionen sind die Beschäftigten hinzuweisen.*
*Ermöglicht die Auswertung der Protokolldaten eine Verhaltens- und Leistungskontrolle, ist sie mitbestimmungspflichtig. Es empfiehlt sich deshalb, eine Vereinbarung mit dem Personalrat abzuschließen, in der die zulässigen Protokollierungen, ihre Aufbewahrungsdauer sowie die Art ihrer Auswertung und ihrer sonstigen Nutzung genau definiert sind. Gegenstand der Vereinbarung ist die Regelung der Mitbestimmungsrechte der Personalräte nach § 67 Abs. 1 Nr. 2 Niedersächsisches Personalvertretungsgesetz (NPersVG) bei der „Einführung und Anwendung technischer Einrichtungen, die geeignet sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen" sowie nach § 67 Abs. 1 Nr. 6 NPersVG bei der „Einführung grundlegend neuer Arbeitsmethoden". Durch eine Vereinbarung mit dem Personalrat sollte daher sichergestellt sein, dass das Instrument der Protokollierung nicht zweckentfremdet verwendet wird.)*

#### 4.4.1 Art und Umfang von Protokollierungen

Bevor Art und Umfang von Protokollierungen festgelegt werden, haben die Daten verarbeitenden

Stellen zu ermitteln, welche gesetzlichen Regelungen für ihren Zuständigkeitsbereich welche Rahmenbedingungen definieren. Die Protokollierung stellt keine Maßnahme im Rahmen des Ermessens dar, sondern ist eine Folge aus den jeweils gültigen gesetzlichen Bestimmungen.

### 4.4.2 Einsichtnahme in die Protokolle

Protokolle, die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen erstellt werden, dürfen nur gemeinsam von Administratoren, Schulleitung und dem behördlichen Datenschutzbeauftragten eingesehen werden. Weitergehende gesetzliche Befugnisse (z.B. Auskunfts- und Einsichtsrechte des Landesbeauftragten für den Datenschutz und der Strafverfolgungsbehörden oder Beteiligungsrechte der Personalvertretung) bleiben unberührt.

### 4.4.3 Aufbewahrungsdauer für Protokolle

Die Aufbewahrungsdauer der Protokolle richtet sich, da es sich um personenbezogene Daten handelt, nach den allgemeinen Löschungsregeln der Datenschutzgesetze. Maßgeblich ist die „Erforderlichkeit zur Aufgabenerfüllung“. Gibt es keinen zwingenden Grund für das weitere Vorhalten von Protokolldateien, besteht eine Löschungspflicht (§ 17 NDSG).
*(Hinweis: Eine exakte Bestimmung des Aufbewahrungszeitraums für Protokolle, deren Auswertung zeitlich nicht konkretisiert ist (z. B. die Protokolle im Zusammenhang mit der Administration), ist nicht möglich.*
*Als Anhaltspunkte können dienen:*

- *die Wahrscheinlichkeit, dass Unregelmäßigkeiten (noch) aufgedeckt werden können und*
- *die Möglichkeit, die Gründe von Unregelmäßigkeiten anhand der Protokolle und anderer Unterlagen aufdecken zu können.*

*Erfahrungsgemäß sollte eine Frist von einem halben Jahr nicht überschritten werden.*
*Soweit Protokolle zum Zwecke gezielter Kontrollen angefertigt werden, z. B. Versuche unbefugten Einloggens sowie die Überschreitung von Befugnissen bzw. Eindringversuche an einer Firewall zu ermitteln, kommen auch mitunter wesentlich kürzere Speicherungsfristen in Betracht. In der Regel reicht hier eine Aufbewahrung bis zur tatsächlichen Kontrolle. Gerade bei diesen Beispielen kommt es auf eine sehr zeitnahe Auswertung mit entsprechenden Reaktionen an.*
*Eine Begrenzung der Speicherungsdauer von Protokolldaten kann auch dadurch erreicht werden, dass durch eine physische "Ringspeicherung" nur eine maximale Anzahl von Protokolldatensätzen für die Kontrolle vorgehalten wird (z. B. die jeweils letzten "n" Sätze).*

### 4.4.4 Maßnahmen bei Verstößen

Ein vorsätzlicher, schwerwiegender Verstoß gegen den Datenschutz oder diese Dienstanweisung kann zum Entzug der Administratoren-Befugnis führen und darüber hinaus Konsequenzen dienst- oder strafrechtlicher Art nach sich ziehen. Dies gilt ebenso bei Verstößen gegen sonstige Vorschriften:

| | |
|---|---|
| § 97b Abs. 2 i. V. m. §§ 94 bis 97 StGB | Verrat in irriger Annahme eines illegalen Geheimnisses, |
| § 120 Abs. 2 StGB | Gefangenenbefreiung |
| § 133 Abs. 3 StGB | Verwahrungsbruch |
| § 184b StGB | Verbreitung, Erwerb und Besitz kinderpornographischer Schriften |
| § 201 Abs. 3 StGB | Verletzung der Vertraulichkeit des Wortes |
| § 202 StGB | Verletzung des Briefgeheimnisses |
| § 202 a bis c StGB | Ausspähen und Abfangen von Daten sowie die Vorbereitung dieser Straftaten |
| § 203 Abs. 2, 4, 5 StGB | Verletzung von Privatgeheimnissen, |

| | |
|---|---|
| § 204 StGB | Verwertung fremder Geheimnisse, |
| § 303b StGB | Computersabotage |
| §§ 331, 332 StGB | Vorteilsannahme und Bestechlichkeit, |
| § 353 b StGB | Verletzung des Dienstgeheimnisses und einer besonderen Geheimhaltungspflicht, |
| § 355 StGB | Verletzung des Steuergeheimnisses |
| § 358 StGB | Nebenfolgen |
| § 35 SGB I i.V.m. §§ 67 bis 85 SGB X | Bestimmungen zum Schutz der Sozialdaten |

**Hinweise zur Schweigepflicht (vgl. u. a. folgende Rechtsvorschriften):**
§ 5 Niedersächsisches Datenschutzgesetz (NDSG)
§ 37 Beamtenstatusgesetz (BeamtStG)
§ 46 Niedersächsisches Beamtengesetz (NBG)
§ 3 Abs. 1 Tarifvertrag für den öffentlichen Dienst (TVöD)
§ 5 Tarifvertrag für Auszubildende des öffentlichen Dienstes (TVAöD)
§ 3 Abs. 2 Tarifvertrag für den öffentlichen Dienst der Länder (TV-L)
§ 9 Niedersächsisches Personalvertretungsrecht (NPersVG)
§§ 40, 43, 54 Abs. 3, 57 Abs. 4, 91 Abs. 4 Niedersächsisches Kommunalverfassungsgesetz (NKomVG)
sowie

- den Beschluss des Landesministeriums zur Schweigepflicht der Beamten, Angestellten und Arbeiter im Landesdienst vom 7. Februar 1984 (Nds. MBl. S. 254, VORIS 20411 01 00 00 023)
- den Gem. RdErl. d. MI, d. StK u. d. übr. Min. vom 6. November 2001 (Nds. MBl. S. 853, VORIS 20600 00 00 00 006)

Der Personalrat hat an der Erstellung dieser Dienstanweisung mitgewirkt.

Diese Dienstanweisung tritt am … in Kraft.
Sie ist von jedem Mitarbeiter, der mit der Administration beauftragt wird, zu beachten. Ihre Kenntnisnahme ist mit einer Bescheinigung zu dokumentieren, bevor er die IT-Systeme und IT-Dienste administrieren darf. Die Bescheinigung ist zu den Personalakten zu nehmen.
Nach spätestens 3 Jahren ist eine erneute Bestätigung erforderlich.

Die Dienstanweisung ... vom ... wird mit gleichem Datum aufgehoben.

..., den .....

_____
Schulleitung

Hiermit bestätige ich, dass ich die „Dienstanweisung für die Administratoren der IT-Systeme und IT-Dienste bei der Musterschule“ erhalten und zur Kenntnis genommen habe.

| | |
|---|---|
| _____ | _____ |
| Ort, Datum | Unterschrift |