Für die Berufsbildende Schule Lahnstein wird folgende

Allgemeine Dienstanweisung über die Maßnahmen zum technischen und organisatorischen Datenschutz

erlassen:

Teil A
ALLGEMEINES

1. Diese Dienstanweisung enthält nähere Bestimmungen über den technisch-organisatorischen Datenschutz
   - bei der Verarbeitung von Daten in automatisierten Verfahren (Teil B)
   - bei der Nutzung von Internet- und E-Mail-Diensten (Teil C)
   - bei der Nutzung von Telefax-Geräten (Teil D)
   - bei der Verarbeitung von Daten in Akten (Teil E)
   - über die Bestellung und die Aufgaben des behördlichen Datenschutzbeauftragten – behDSB – (Teil F).

   Unter Verfahren ist eine definierte Aufgabe zu verstehen, zu deren Erfüllung personenbezogene Daten in einer oder mehreren Dateien verarbeitet werden.
   Die Dienstanweisung ist von allen Bediensteten, die personenbezogene Daten im Sinne des § 3 Abs.1 LDSG verarbeiten, zu beachten. Soweit weitere oder von den nachfolgenden Bestimmungen abweichende Maßnahmen für einzelne Anwendungen erforderlich sind, werden diese für die jeweilige Anwendung schriftlich festgelegt. Diese und alle sonstigen zu speziellen Inhalten mit Datenschutzbezug getroffenen Dienstanweisungen bleiben von der vorliegenden Dienstanweisung unberührt.

2. Bedienstete, die personenbezogene Daten verarbeiten, sind nach § 8 LDSG unter Verwendung des als **Anlage 1** angefügten Vordrucks auf die Einhaltung des Datengeheimnisses zu verpflichten. Die Verpflichtung erfolgt durch die Schulleitung der Berufsbildenden Schule Lahnstein.

3. Sofern Daten ohne Kenntnis der Betroffenen erhoben werden und eine Benachrichtigungspflicht nach § 18 Abs. 1 LDSG besteht, hat die Benachrichtigung in Abstimmung mit dem behDSB zu erfolgen. Bei der Festlegung von Ausnahmen nach § 18 Abs. 2 LDSG wirkt dieser mit.

4. Anträge auf Auskunft nach § 18 Abs. 3 LDSG sind über den behDSB der Schulleitung der Berufsbildenden Schule Lahnstein zuzuleiten, die über die weitere Behandlung entscheidet.

5. Der behDSB ist in allen Angelegenheiten, die den Datenschutz und insbesondere den technischen und organisatorischen Datenschutz betreffen, beratend hinzuzuziehen. Auch im Hinblick auf das in §5 Abs. 5 LDSG festgelegte Verbot einer automatisierten Einzelentscheidung sowie die möglicherweise bestehende Pflicht zur Durchführung einer Vorabkontrolle nach § 9 Abs. 5 LDSG ist er bei der Entwicklung, Einführung und Änderung von Verfahren frühzeitig zu beteiligen (vgl. §11 Abs. 3 Nr. 1 LDSG).

Teil B
DATENVERARBEITUNG IN AUTOMATISIERTEN VERFAHREN

1 <u>Generelle Regelungen</u>

1.1 Auswahl, Einsatz und Entwicklung von automatisierten Verfahren; Datensicherung

1.1.1 Bei der Auswahl und Entwicklung von automatisierten Verfahren ist darauf zu achten, dass bei ihrer Anwendung der Umfang der zu erhebenden, zu verarbeitenden oder zu nutzenden perso-

nenbezogenen Daten auf ein Minimum beschränkt wird (Grundsatz der Datenvermeidung und der Datensparsamkeit, § 1 Abs. 3 LDSG).

1.1.2 Änderungen an der Konfiguration der eingesetzten Systeme sind grundsätzlich nur durch die Systembetreuung zulässig.

1.1.3 Die Verwendung privater Hard- und Software im Netzwerk der Schule bedarf der schriftlichen Genehmigung der Schulleitung. Hiervon ausgenommen ist das Verwenden externer Speichermedien.

1.1.4 Datenbestände sind in regelmäßigen Zeitabständen so zu sichern, dass sie im Fall des Verlusts oder der Zerstörung mit vertretbarem Aufwand wiederhergestellt werden können. Nähere Bestimmungen über die Art und Weise der Sicherung trifft die Schulleitung.

1.2 Zutritt zu Räumen

1.2.1 Räume, in denen sich Datenverarbeitungsgeräte oder Datenträger befinden, sind bei Abwesenheit grundsätzlich zu verschließen. Bei Unterbrechung oder Beendigung der Bildschirmarbeit und Verlassen der Diensträume ist die unbefugte Nutzung durch Sperrung oder Abmeldung der Geräte zu verhindern.
Räume mit zentralen Einrichtungen der Informationstechnik (z.B. Netzwerk-Server, DFÜ-Anschlüsse) sind bei Abwesenheit immer zu verschließen.

2 Unterrichtsnetzwerk

2.1 Allgemeine Grundsätze

2.1.1 Im Unterrichtsnetzwerk werden keine personenbezogenen Daten (Zeugnisse, Verweise, benotete Leistungsnachweise o.ä.) gespeichert.

2.1.2 Sollten unterrichtsbedingt personenbezogene Daten (Lebensläufe, Bewerbungsschreiben o.ä.) entstehen, so sind diese umgehend auf externe Datenträger in der Verantwortung der Betroffenen auszulagern.

2.2 Benutzerverwaltung; Passwortvergabe

2.2.1 Für jeden autorisierten Benutzer ist eine Benutzerkennung einzurichten und ein Anfangspasswort zuzuweisen. Dieses ist bei der ersten Anmeldung durch den Anwender sofort zu ändern. Sofern möglich, ist diese Änderung automatisiert vorzugeben. Im System ist ein Zeitraum einzustellen, nach dessen Ablauf das Passwort zwingend geändert werden muss.

2.2.2 Passwörter sind in regelmäßigen Zeitabständen durch den Nutzer selbst zu ändern. Weitere Regeln hinsichtlich der Passwortgestaltung sind aus der **Anlage 3** zu entnehmen.

2.3 Protokollierung

2.3.1 Die Nutzung der Datenverarbeitungssysteme wird mit den Angaben über die Benutzer, Zeitpunkt der An- und Abmeldung sowie ggf. fehlerhafte Zugriffsversuche protokolliert.

2.3.2 Die Protokolldaten dürfen gemäß § 13 Abs. 6 LDSG nur zu Zwecken der Datenschutzkontrolle, der Datensicherung und zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage genutzt werden. Ihre Verwendung für allgemeine Leistungs- und Verhaltenskontrollen ist nach § 31 Abs. 5 LDSG ausdrücklich untersagt.

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

3 Verwaltungsnetzwerk

3.1 Auswahl, Einsatz und Entwicklung von automatisierten Verfahren; Datensicherung

3.1.1 Die vorhandene IT-Infrastruktur und die eingesetzten Verfahren sind fortlaufend zu erfassen und hinsichtlich ihres Schutzbedarfs zu bewerten.

3.1.2 Bei der Auswahl und Entwicklung von automatisierten Verfahren müssen die technischen Voraussetzungen vorhanden sein, um künftigen Auskunftsersuchen nach § 18 Abs. 3 LDSG entsprechen zu können.

3.2 Dokumentation

3.2.1 Für jedes automatisierte Verfahren ist durch die Schulleitung eine Verfahrensbeschreibung zu erstellen und fortzuschreiben. Hierfür sind die Seiten 3 und 4 des beigefügten Vordrucks (**Anlage 2**) zu verwenden. Sie dienen als Grundlage für das Verfahrensverzeichnis (§ 10 Abs. 2 LDSG) und für die Anmeldung zum Datenschutzregister. Das Verfahrensverzeichnis wird vom behDSB geführt. Die nach § 10 Abs. 2 LDSG hierzu erforderlichen Angaben, insbesondere die Verfahrensbeschreibung, sind von der Organisationseinheit, in der das Verfahren eingesetzt wird, dem behDSB zuzuleiten. Anträge auf Einsicht in das Verfahrensverzeichnis nach § 10 Abs. 4 LDSG sind direkt an den behDSB zu richten.

3.2.2 Werden sensitive personenbezogene Daten in komplexen Verfahren verarbeitet, sind die wesentlichen Verarbeitungsschritte und die daran beteiligten Stellen fortlaufend schriftlich zu dokumentieren. Die Dokumentation ist dem behDSB auf Anforderung zur Verfügung zu stellen.

3.3 Beteiligung des Landesbeauftragten für den Datenschutz

3.3.1 Die Anmeldung beim Landesbeauftragten für den Datenschutz nach § 27 Abs. 1 LDSG erfolgt durch den behDSB unter Verwendung des vorgesehenen Vordrucks (vgl. **Anlage 2**).

3.3.2 Bei der Einrichtung eines automatisierten Übermittlungsverfahrens gemäß § 7 LDSG ist auf die rechtzeitige Beteiligung des LfD zu achten. Zu diesem Zwecke ist der behDSB frühzeitig von der beabsichtigten Einrichtung eines solchen Verfahrens zu unterrichten.

3.4 Zutritt zu Räumen

3.4.1 Zu den Räumen, in denen sich zentrale Einrichtungen der Datenverarbeitung befinden, dürfen nur die ausdrücklich bestimmten Bediensteten Zutritt haben. Reinigungs-, Wartungs- und ähnliche Aufgaben dürfen nur in Anwesenheit dieser Bediensteten durchgeführt werden.

3.4.2 Bildschirmgeräte sind so aufzustellen, dass sie von Unbefugten nicht eingesehen werden können.

3.5 Benutzerverwaltung; Passwortvergabe

3.5.1 Für jeden autorisierten Benutzer ist eine Benutzerkennung einzurichten und ein Anfangspasswort zuzuweisen. Dieses ist bei der ersten Anmeldung durch den Anwender sofort zu ändern. Sofern möglich, ist diese Änderung automatisiert vorzugeben. Im System ist ein Zeitraum einzustellen, nach dessen Ablauf das Passwort zwingend geändert werden muss.

3.5.2 Passwörter sind in regelmäßigen Zeitabständen durch den Nutzer selbst zu ändern. Weitere Regeln hinsichtlich der Passwortgestaltung sind aus der **Anlage 3** zu entnehmen.

3.6 Beschränkung von Zugriffsmöglichkeiten; Zugriffsrechteverwaltung

3.6.1 Zugriffsmöglichkeiten auf personenbezogene Daten sind auf den für die Aufgabenerfüllung erforderlichen Umfang zu beschränken. Die Schulleitung bestimmt und dokumentiert, welche Bedienstete in welchem Umfang autorisiert sind, Daten einzugeben, zu lesen, zu verändern und zu löschen.

3.6.2 Personenbezogene Daten, die gegenüber der Systembetreuung und Personen mit erweiterten Zugriffsrechten auf den Datenverarbeitungssystemen vertraulich zu halten sind (z.B. Personal-, Sozial- oder Gesundheitsdaten), sind in angemessener Form kryptografisch zu verschlüsseln. Die notwendigen technischen Lösungen sind durch die Systembetreuung zur Verfügung zu stellen.

3.6.3 Soweit Lehrkräfte personenbezogene Daten zu dienstlichen Zwecken auf einem privaten Computer verarbeiten, ist dies nur mit Einwilligung der Schulleitung zulässig. Hierzu hat die Lehrkraft schriftlich zu versichern, dass bei der Verarbeitung dieser Daten alle relevanten Datenschutzbestimmungen beachtet werden und dass das private Datenverarbeitungsgerät unter den gleichen Bedingungen wie dienstliche Geräte kontrolliert werden kann.

3.6.4 Für die Einrichtung automatisierter Direktabrufverfahren ist § 7 LDSG zu beachten. Vor der Erweiterung von darauf bezogenen Zugriffsrechten sind der behDSB und die Schulleitung zu unterrichten.

3.7 Protokollierung

3.7.1 Die Nutzung der Datenverarbeitungssysteme wird mit den Angaben über die Benutzer, Zeitpunkt der An- und Abmeldung sowie ggf. fehlerhafte Zugriffsversuche protokolliert.

3.7.2 Die Protokolldaten dürfen gemäß § 13 Abs. 6 LDSG nur zu Zwecken der Datenschutzkontrolle, der Datensicherung und zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage genutzt werden. Ihre Verwendung für allgemeine Leistungs- und Verhaltenskontrollen ist nach § 31 Abs. 5 LDSG ausdrücklich untersagt.

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

3.8 Gewährleistung der Zweckbindung

3.8.1 Zu unterschiedlichen Zwecken erhobene Daten müssen getrennt verarbeitet werden können (§ 9 Abs. 2 Nr. 8 LDSG). Dem ist grundsätzlich dadurch zu entsprechen, dass die Verarbeitung in getrennten Verfahren erfolgt. Ist dies nicht möglich oder zweckdienlich, sind die betroffenen Daten in verschiedenen Dateien zu verarbeiten.

3.8.2 Soweit die gemeinsame Speicherung in einer Datei technisch bedingt oder aus sachlichen Gründen geboten ist, sind die Dateien so zu kennzeichnen, dass eine getrennte Verarbeitung möglich ist (Sortiermerkmale, Kennziffern o.ä.).

3.9 Empfang, Versand, Weitergabe

3.9.1 Über Empfang, Versand und Weitergabe von personenbezogenen Daten ist ein Nachweis zu führen. Dieser wird bei der Schulleitung geführt.

3.9.2 Beim externen Versand der Datenträger ist eine ausreichend sichere Versandform zu wählen; gegebenenfalls sind die Daten angemessen zu verschlüsseln. Die interne Weitergabe der Datenträger innerhalb der Dienststelle hat von Hand oder in einem verschlossenen Umschlag zu erfolgen.

3.10 Datenträger

3.10.1 Datenträger sind mit einer Kennzeichnung zu versehen, die mindestens folgende Angaben enthalten muss:
- Behörden- und Organisationsbezeichnung
- eindeutige Kennzeichnung des Datenträgers
- Inhaltsangabe
- Datum der Erstellung bzw. letzten Änderung

3.10.2 Datenträger mit personenbezogenen Daten sind grundsätzlich unter Verschluss zu halten. Dauerhafte Aufbewahrung am Arbeitsplatz ist zulässig, wenn dies in geeigneten Behältnissen (z.B. Datensicherungsschränke) erfolgt. Schreibtische oder einfache Büroschränke sind hierfür regelmäßig nicht geeignet.

3.10.3 Vor der weiteren Verarbeitung von Datenträgern ist sicherzustellen, dass von ihnen keine Gefährdung für automatisierte Verfahren ausgeht (Virenprüfung).

3.10.4 Nicht mehr benötigte Datenträger sind zu löschen oder ordnungsgemäß zu entsorgen. Bei der Löschung ist eine Löschdämpfung von mindestens 90 dB einzuhalten (entspricht der Anforderungsstufe B der DIN 33858 (Stand 04/1993) *[siehe Anlage 4]*).

3.11 Löschung, Sperrung und Archivierung

3.11.1 Für jedes Verfahren ist von der Schulleitung ein Zeitraum festzulegen, nach dessen Ablauf die personenbezogenen Daten nach den in § 19 LDSG oder einer vorrangigen Rechtsvorschrift enthaltenen Vorgaben zu löschen oder zu sperren sind. Die Systemadministration ist hiervon zu unterrichten.

3.11.2 Die Verantwortung für die Löschung oder Sperrung der Daten liegt bei der Schulleitung. Diese entscheidet auch in Abstimmung mit der Systemadministration über das konkrete Verfahren. Die allgemeine Anbietungspflicht nach § 7 Abs. 1 Landesarchivgesetz bleibt unberührt.

3.11.3 Personenbezogene Daten abgeschlossener Fälle, die für die laufende Bearbeitung nicht mehr benötigt werden, sind durch die Übernahme in einen gesonderten Datenbestand oder die Vergabe von Zugriffsrechten so zu sichern, dass ein Zugriff nur in begründeten Fällen möglich ist (interne Archivierung).

3.12 Wartung

3.12.1 Wartungsarbeiten an DV-Geräten dürfen nur in Anwesenheit eines verantwortlichen Bediensteten durchgeführt werden.

3.12.2 Auch für das Wartungspersonal ist eine Benutzerkennung mit Passwort zu vergeben. Es ist sicherzustellen, dass diese Kennung nur für Wartungsfälle benutzt werden kann. Die Inanspruchnahme ist zu dokumentieren (z.B. Eintragung in Logbuch, automatische Protokollierung).

3.12.3 Für die Einrichtung eines Verfahrens zur Fernwartung trifft die Schulleitung im Hinblick auf dessen genaue Ausgestaltung nähere Bestimmungen. Der behDSB ist zu beteiligen.

3.13 Datenverarbeitung im Auftrag/ Outsourcing der Datenverarbeitung

3.13.1 Die Verarbeitung personenbezogener Daten im Auftrag durch andere Personen oder Stellen ist bei Beachtung der gesetzlichen Vorgaben, insbesondere der §§ 4 und 9 LDSG, nur mit Zustimmung der Schulleitung zulässig. Der behDSB ist vorher zu hören. Der Vertragsgestaltung sind die Empfehlungen des Landesbeauftragten für den Datenschutz zur Datenverarbeitung im Auftrag zu Grunde zu legen. Weiterhin ist zu prüfen, inwieweit hierfür spezialgesetzliche Regelungen bestehen (z.B. § 80 SGB X, § 36 Abs. 9 Landeskrankenhausgesetz).

Teil C
ORGANISATORISCHE UND TECHNISCHE ASPEKTE DER NUTZUNG VON INTERNET- UND E-MAIL-DIENSTEN

1 <u>Generelle Regelungen</u>

1.1 Grundsätze der Internetnutzung

1.1.1 Die Nutzung des Internets und seiner Dienste ist an der BBS Lahnstein grundsätzlich nur zu unterrichtlichen bzw. dienstlichen Zwecken erlaubt.

1.1.2 Das Aufrufen von Internetseiten, die eine Verletzung religiöser, moralischer, weltanschaulicher oder auch ethischer Empfindungen verursachen können oder die rassistische oder faschistische Äußerungen enthalten bzw. zu Gewalttaten oder kriminellen Delikten auffordern, ist untersagt.

1.1.3 Es ist grundsätzlich verboten, die Internetzugänge der BBS Lahnstein zur Verbreitung von Informationen zu verwenden, die dazu geeignet sind, dem Ansehen der Schule in irgendeiner Weise Schaden zuzufügen.

2 Unterrichtsnetzwerk

2.1 Internet / World Wide Web

2.1.1 Bei der Nutzung des Internets werden neben den Daten der Benutzeranmeldung auch Datum und Uhrzeit des Seitenaufrufs, URL der aufgerufenen Seite und IP-Adresse des aufrufenden Rechners protokolliert. (Hinsichtlich der Einsichtnahme in die Protokolle gilt auch hier Teil B Abschnitt 2.3 dieser Dienstanweisung.)

2.1.2 Empfohlen wird der Einsatz von Vorrichtungen, mit denen die aufsichtsführende Lehrkraft den Bildschirm jedes Schülercomputers auf dem ihrem eigenen Platz sichtbar machen kann.

3 Verwaltungsnetzwerk

3.1 Internet / World Wide Web

3.1.1 Bei der Nutzung des Internets werden neben den Daten der Benutzeranmeldung auch Datum und Uhrzeit des Seitenaufrufs, URL der aufgerufenen Seite und IP-Adresse des aufrufenden Rechners protokolliert. (Hinsichtlich der Einsichtnahme in die Protokolle gilt auch hier Teil B Abschnitt 3.7 dieser Dienstanweisung.)

3.1.2 Dateien mit Anhängen sind vor einer Übernahme ins Verwaltungsnetz sorgfältig auf Viren und sonstige unerwünschte Nebenwirkungen hin zu untersuchen.

3.1.3 Es darf keine nach außen bekannte IP-Adresse verwendet werden.

3.1.4 Der Verwaltungscomputer mit Internetzugang muss mit einem eigenen Passwort vor unbefugter Inbetriebnahme geschützt werden.

3.1.5 Aktive Elemente (Active-X, Java, Java-Script) dürfen im Web-Browser generell nur nach einer Bestätigung durch die Anwenderin oder den Anwender ausgeführt werden. Die Ausführung von Active-X-Elementen sollte aus Sicherheitsgründen generell unterbunden werden.

3.1.6 Es sollte ein Provider mit dynamischer IP-Adressenverwaltung ausgewählt werden.

3.1.7 Der Zugriff sollte programmmäßig auf als sicher bekannte Adressen beschränkt werden

3.1.8 Der gesamte Datenverkehr zwischen Internet und Verwaltungsbereich ist durch eine Virenscanner- bzw. Firewallsoftware zu prüfen, die durch Aktualisierungen jederzeit auf dem aktuellen Stand gehalten werden müssen.

3.1.9 Der gesamte Datenverkehr zwischen Internet und Verwaltungsbereich (also alle tatsächlichen und alle versuchten Zugriffe von innen und außen) sollte protokolliert werden; diese Protokolle sollten gezielt stichprobenweise sowie anlassbezogen (z. B. bei Verdacht auf missbräuchliche oder sicherheitsgefährdende Nutzung des Internet-Zugangs) überprüft werden. Die am Verwaltungscomputer arbeitenden Personen sind darüber zu informieren

3.2 E-Mail

3.2.1 Die Mail-Adresse innerhalb des EPOS-Systems lautet <Schulnummer>@sl.Bildung-rp.de. Diese Adresse kann anderen Behörden und sonstigen Stellen mitgeteilt werden.

3.2.2 E-Mails mit Anhängen einer oder eines nicht als sicher bekannten und zuverlässig identifizierten Absenderin oder Absenders dürfen nicht geöffnet werden. (Vor einer anschließenden Übernahme ins Verwaltungsnetz sind Anhänge sorgfältig auf Viren und sonstige unerwünschte Nebenwirkungen hin zu untersuchen.)

3.2.3 Die eingesetzten Programme für die E-Mail-Nutzung sind so zu konfigurieren, dass erfolgreich empfangene Nachrichten auf dem Mailserver des Providers gelöscht werden.

3.2.4 Im Rahmen der dienstlichen Nutzung von E-Mail sollten grundsätzlich nur solche Anhänge von E-Mails geöffnet bzw. versandt werden, bei denen davon ausgegangen werden kann, dass es sich um dienstlich benötigte Dokumente handelt.

3.2.5 Der Name im ,,Von"-Feld einer E-Mail ist kein Hinweis auf die Vertrauenswürdigkeit der Nachricht. Ein infiziertes System kann E-Mails im Namen der Anwenderin oder des Anwenders versenden, ohne dass dieser etwas davon bemerkt. Bei Verdacht auf Schadprogramme (,,Viren", ,,Trojanische Pferde" etc.) muss bei der Absenderin oder dem Absender der E-Mail nachgefragt oder die verantwortliche Person verständigt werden.

3.2.6 Bei der Versendung eines Dokuments soll dessen Inhalt im ,,Betreff" sachgerecht umschrieben werden. In Schreiben und vergleichbaren elektronischen Dokumenten sollen die Anschrift bzw. die empfangende Stelle als Text in das entsprechende Schriftstück aufgenommen werden.

3.2.7 Datenformate, die nicht allgemein gebräuchlich sind, sollen nur dann als Anlage versandt werden, wenn bekannt ist, dass die empfangende Stelle dieses Datenformat verarbeiten kann. Die einem elektronischen Dokument beigefügten Anlagen sind in dem Anschreiben einzeln aufzuführen, um der empfangenden Stelle eine Überprüfung der Anzahl und des Formats der Anlagen zu ermöglichen.

3.2.8 Umfangreiche Anlagen sollen komprimiert werden, soweit bei der empfangenden Stelle eine Dekomprimierung möglich ist.

3.2.9 Beim Versand elektronischer Post (E-Mail) kann grundsätzlich eine Empfangs- sowie eine Lesebestätigung angefordert werden. Diese ,,automatischen" Bestätigungen werden jedoch nicht von allen Systemen unterstützt. Für den Nachweis einer ordnungsgemäßen Zustellung soll deshalb im Zweifelsfalle von der Empfängerin oder vom Empfänger eine Nachricht mit der ausdrücklichen Bestätigung des Eingangs angefordert werden.

3.2.10 Löst ein Schreiben eine unmittelbare Rechtswirkung aus oder ist es von besonderer Bedeutung, so ist es mit der elektronischen Signatur gemäß dem Gesetz über Rahmenbedingungen für elektronische Signaturen zu versehen, soweit eine solche Funktion vorhanden ist.

3.2.11 Elektronische Dokumente sind auszudrucken und in Papierform zu den entsprechenden Akten zu nehmen, soweit dies zur Erfüllung der Aufgaben erforderlich ist, auch wenn der Vorgang anschließend elektronisch bearbeitet wird. Auf dem für die Akten bestimmten Ausdruck des Dokuments (Entwurf) ist handschriftlich die Versendungsart, das Datum und das Namenszeichen der oder des absendenden Bediensteten zu vermerken. Beim Versand elektronischer Dokumente kann auch die elektronische Absendebestätigung ausgedruckt und zu den Akten genommen werden. Im Falle der Notwendigkeit des Nachweises des Zugangs eines elektronisch versandten Dokuments soll außerdem die automatische Zugangsbestätigung ausgedruckt und zu den Akten genommen werden.

3.2.12 Das elektronische Postfach ist regelmäßig, mindestens jedoch einmal täglich, auf eingegangene E-Mails zu überprüfen.

3.2.13 Im Falle der längeren Abwesenheit einer Mitarbeiterin oder eines Mitarbeiters ist in der E-Mail-Anwendung die Funktion des Abwesenheitsassistenten zu aktivieren. Falls diese Funktion technisch bedingt nicht genutzt werden kann, ist das elektronische Postfach von einer Vertreterin oder einem Vertreter regelmäßig auf eingegangene E-Mails zu überprüfen.

3.2.14 Der E-Mail-Dienst und der PC-Fax-Dienst dürfen für die Versendung von allen in digitaler Form vorliegenden Informationen wie Texten, Daten, Tabellen, Grafiken genutzt werden, soweit nicht technische oder rechtliche Gründe wie beispielsweise das Erfordernis einer eigenhändigen Unterschrift entgegenstehen.

3.2.15 Für Verschlusssachen gelten die Regelungen der Verschlusssachenanweisung. Danach sind die Verschlusssachen bei der Übertragung über technische Kommunikationsverbindungen mit zugelassenen Verfahren zu kryptieren bzw. durch andere zugelassene Maßnahmen zu sichern.

3.2.16 Für die elektronische Post an Schulleitungen bleiben Regelungen für die Nutzung des EPOS-Netzwerkes unberührt.

3.2.17 Für die Nutzung des PC-Fax-Dienstes gelten die Bestimmungen für die Mail-Nutzung gleichermaßen.

Teil D
NUTZUNG VON TELEFAX-GERÄTEN

1. Bei der Versendung von Telefax-Schreiben ist ein Vorblatt zu verwenden, aus dem der Absender, dessen Telefax- und Telefonnummer sowie die Anzahl der gesendeten Seiten ersichtlich ist, es sei denn, der sichere Zugang ist anderweitig gesichert.
2. Das Versenden eines Schreibens ist durch ein Protokoll oder einen Verifikationsstempel auf dem Original nachzuweisen und in der entsprechenden Akte zu dokumentieren. Werden mehrere Seiten als Telefax-Schreiben versandt, sind diese durchzunummerieren.

3. Besonders schutzwürdige personenbezogene Daten (z. B. Angaben, die dem Steuer-, Sozial-, Arzt- oder dem Personalaktengeheimnis unterliegen) sollen nur dann per Telefax versendet werden, wenn die Übermittlung dieser Daten besonders eilbedürftig ist und zusätzliche Datensicherungsmaßnahmen getroffen werden (Absprache des Zeitpunktes der Versendung mit dem Empfänger, Bestätigung des Erhalts der Sendung durch den Empfänger).
4. Die für die Entgegennahme und die Weiterleitung zuständigen Bediensteten haben sicherzustellen, dass eine Kenntnisnahme durch Unbefugte ausgeschlossen ist.
5. Der Eingang von Telefax-Schreiben soll durch entsprechende Empfangsprotokolle dokumentiert werden. Diese sind gesichert aufzubewahren und gegen unbefugte Einsichtnahme zu schützen.

Teil E
AKTENVERARBEITUNG

1. Akten sind grundsätzlich unter Verschluss aufzubewahren.
2. Es sind Maßnahmen zu treffen, die verhindern, dass Akten bei der Verarbeitung von Unbefugten eingesehen oder entwendet werden können.
3. Die Aufbewahrung und Archivierung von Schriftgut richtet sich nach der Verwaltungsvorschrift des Kultusministeriums „Aufbewahrung, Aussonderung, Archivierung und Vernichtung des amtlichen Schriftgutes“ vom 6. März 1986 (Amtsblatt S. 227) sowie die zugehörige Bekanntmachung vom 25. August 1986 (Amtsblatt S. 483).
4. Für die Vernichtung amtlichen Schriftgutes wird ein Unternehmen beauftragt, das eine ordnungsgemäße Vernichtung vorzunehmen hat.
5. Nicht benötigtes Schriftgut ist zeitnah zu vernichten. Soweit Schriftgut bis zur Vernichtung gesammelt wird, ist sicherzustellen, dass Unbefugte keine Kenntnis nehmen können. Bei der Beschaffung von Geräten zur Aktenvernichtung sind die Anforderungen nach DIN 32757 (Stand 01/1995) Stufe 3 oder höher [siehe Anlage 5] einzuhalten.

Teil F
DER BEHÖRDLICHE DATENSCHUTZBEAUFTRAGTE

1. Der behDSB darf bei Ausübung seiner Funktion als Datenschutzbeauftragter nicht in einer Interessenkollision zu seinen sonstigen regelmäßig von ihm wahrzunehmenden Aufgaben stehen. Deshalb dürfen ihm keine Aufgaben aus den Bereichen Organisation, IT -Administration oder Anwendungsbetreuung übertragen sein, soweit er dadurch als behDSB seine eigene Tätigkeit beurteilen müsste. Die Bestellung und Abberufung des behDSB unterliegen der Mitbestimmung des Personalrates (§ 80 Abs. 1 Nr. 11 LPersVG).
2. Der behDSB ist in der Wahrnehmung dieses Amtes organisatorisch keiner Verwaltungseinheit (Abteilung oder Referat) zugeordnet, sondern unmittelbar der Behördenleitung unterstellt. Er ist bei Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei und darf wegen der Erfüllung seiner Aufgaben nicht benachteiligt werden.
3. Gegenüber der Dienststellenleitung hat er ein direktes Vortragsrecht.
4. Er ist bei der Erfüllung seiner Aufgaben zu unterstützen. Ihm ist insbesondere Kenntnis vom Schriftverkehr mit dem Landesbeauftragten für den Datenschutz zu geben.

5. <u>Der behDSB hat folgende Aufgaben:</u>
   - Er unterstützt die Dienststelle bei der Gewährleistung des Datenschutzes, insbesondere bei der Durchführung der Maßnahmen des technischen und organisatorischen Datenschutzes.
   - Bei der Einführung und Anwendung von Verfahren, in denen personenbezogene Daten automatisiert verarbeitet werden, wirkt er auf die Einhaltungen der Datenschutzvorschriften und insbesondere dieser Bestimmungen hin (§ 11 Abs. 3 Nr. 1 LDSG). Deshalb ist er über die Einrichtung und Änderung sämtlicher Vorhaben der automatisierten Verarbeitung personenbezogener Daten rechtzeitig zu unterrichten.

- Er hat zu prüfen, ob automatisierte Verfahren gegen das Verbot automatisierter Einzelentscheidungen nach § 5 Abs. 5 LDSG verstoßen und ob im Falle einer Datenerhebung ohne Kenntnis der Betroffenen für die verantwortliche Stelle eine Benachrichtigungspflicht nach § 18 Abs. 1 LDSG besteht.
- Er hat die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften des LDSG, den hierzu ergangenen Verordnungen und Vorschriften sowie mit dieser Dienstanweisung vertraut zu machen (§ 11 Abs. 3 Nr. 2 LDSG).
- Er führt Vorabkontrollen nach § 9 Abs. 5 LDSG durch (§ 11 Abs. 3 Nr. 3 LDSG).
- Er führt das Verfahrensverzeichnis und macht es auf der Grundlage des § 10 Abs. 4 LDSG jedermann in geeigneter Weise verfügbar (§ 11 Abs. 3 Nr. 4 LDSG).
- Er gibt Hinweise und Empfehlungen zur Umsetzung und Beachtung dieser und anderer Bestimmungen über den Datenschutz (§ 11 Abs. 3 Nr. 5 LDSG). Er ist deshalb bei Zweifelsfragen, die die Anwendung des LDSG, anderer Vorschriften zum Datenschutz und dieser Dienstanweisung betreffen, zu beteiligen.
- Er steht den Betroffenen in allen datenschutzrechtlichen Angelegenheiten, soweit sie die Berufsbildende Schule Lahnstein betreffen, als Ansprechpartner zur Verfügung (§ 11 Abs. 5 Satz 2 LDSG).
- Er hat darauf hinzuwirken, dass die bei der Verarbeitung personenbezogener Daten tätigen Personen gemäß den datenschutzrechtlichen Bestimmungen auf das Datengeheimnis verpflichtet werden.
- Er wirkt darauf hin, dass nach Teil B.VII dieser Dienstanweisung die im Rahmen der Durchführung der technischen und organisatorischen Maßnahmen erstellten Protokolle in regelmäßigen Abständen auf eventuell vorhandene Unregelmäßigkeiten überprüft werden. Die Prüfung der Protokolle ist von dem behDSB zu dokumentieren.

Teil G
SCHLUSSBESTIMMUNGEN

1. **Meldepflicht**
   Alle sicherheitsrelevanten Ereignisse (wie z. B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste und Daten, Verdacht auf Missbrauch der eigenen Kennworte usw.) sind sofort der verantwortlichen Person zu melden.

2. **Sanktionen**
   Verstöße gegen diese Dienstanweisung und die sonstigen geltenden Regelungen und Vorschriften hinsichtlich der Anwendung von Informationstechnik können dienstliche Konsequenzen haben.

3. **Einschränkungen**
   Die nachfolgend genannten Punkte dieser Dienstanweisung werden erst umgesetzt, wenn auch das Verwaltungsnetzwerk im Rahmen einer Fremdwartung betreut wird:
   Teil B: 3.4.1 / 3.5 / 3.6.2 / 3.7.1 Teil C: 3.1.1 / 3.1.7 / 3.1.8 / 3.1.9 / 3.2.3

Inkrafttreten

Diese Dienstanweisung tritt zum 01. Dezember 2008 in Kraft. Gleichzeitig tritt die Dienstanweisung vom 29. Oktober 1993 außer Kraft.