Erlass über IT-Sicherheit und Datenschutz in Schulverwaltungen, zur Nutzung von E-Mail und zur Erhebung und Veröffentlichung interner Daten

Erlass vom 27. November 2009 Z.5 - 640.000.005-0000 Gült. Verz. Nr. 7200 (ABl. 1/10)

Grundsätze

Im Rahmen der Erfüllung ihres gesetzlichen Auftrages ist die einzelne Schule veranlasst, eine Fülle von Informationen und Daten über Schülerinnen und Schülern, Lehrkräfte, Eltern aber auch über die Unterrichtsorganisation vorzuhalten, zu speichern und zu verarbeiten. Dies geschieht zunehmend nicht mehr nur in der herkömmlichen Form von Listen, Akten und Klassenbüchern, sondern auch in elektronischer Form, vor allem im Rahmen der Lehrer- und Schülerdatenbank (LUSD) oder der Nutzung elektronischer Dokumente und Tabellen. Die Rechtmäßigkeit der Haltung und Verarbeitung solcher Daten ist vor allem durch das Hessische Schulgesetz (z. B. § 83 Abs. 1 Satz1) sowie die Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen vom 4. Februar 2009 begründet, aber auch begrenzt. Um das informationelle Selbstbestimmungsrecht der Beteiligten zu schützen, sind im Besonderen die Vorgaben des Hessischen Datenschutzgesetzes (HDSG) und hier besonders die Anforderungen an die IT-Sicherheit zu beachten. Dieser Erlass konkretisiert die Anforderungen unter besonderer Berücksichtigung der Verhältnisse in den einzelnen Schulen bzw. den Schulsekretariaten.

1. Aufklärungspflichten beim Erheben von Daten (§ 12 Abs. 4 HDSG)

Schulen erhalten die ersten personenbezogenen Daten von Schülern und Eltern bei der Erstanmeldung der Schülerin oder des Schülers an einer hessischen Schule. Soweit sie nicht aus den Systemen der Meldeämter übermittelt werden, erhebt die Schule die Daten bei Eltern und Schülern. Bei der Datenerhebung sind die Eltern bzw. die volljährigen Schüler auf die Tatsache hinzuweisen, dass diese Daten sowie weitere Daten, die im Rahmen des Schulbesuches entstehen und zu Dokumentation des Bildungsweges des Kindes notwendig sind, in der Schule gespeichert und verarbeitet werden (Aufklärungspflicht). Welche Daten dieses zunächst sind, regelt die „Verordnung zur Verarbeitung personenbezogener Daten in Schulen und Statistiken in Schulen vom 4. Februar 2009“. Darüber hinausgehende Daten können die Schulen nur verarbeiten, wenn sie bei den Betroffenen und mit deren Zustimmung und Kenntnis erhoben wurden. Diese Einwilligung bedarf der Schriftform (§ 7 Abs. 1 Nr. 3 HDSG). (s. hierzu den Erlass „Information von Eltern und volljährigen Schülerinnen und Schülern über die Datenverarbeitung in der Schule, Erlass vom 19.10.2009 [ABl. S. 811], Az.: Z.5 - 000.256. 000-00039“)

2. Maßnahmen zum Schutz personenbezogener Daten

Es muss in der Schule sichergestellt sein, dass nur solche Personen Zugriff auf die in der Schule gespeicherten personenbezogenen Daten erhalten, bei denen für den Zugriff eine dienstliche Notwendigkeit besteht und die hierzu auch eine Befugnis haben. Dies gilt für Daten die in konventionellen Akten gehalten werden gleichermaßen wie für Zugriffe auf Daten in einem IT-Verfahren, zum Beispiel der LUSD. Dies bedeutet, dass Lehrkräfte grundsätzlich eine Zugangsberechtigung nur zu Daten der Schüler besitzen die sie unterrichten, nicht aber zu allen Schülern der Schule. Besteht eine pädagogische Notwendigkeit, Information über andere Schüler zu erhalten, so ist das Ersuchen an den zuständigen Klassenlehrer/Klassenlehrerin oder Tutor/Tutorin oder an die Schulleitung zu richten.

3. Zuständigkeiten

Nach § 88 HSchG ist der Schulleiter gegenüber möglichen Betroffenen, dem Hessischen Kultusministerium und dem jeweiligen Schulträger dafür verantwortlich, dass allen datenschutzrechtlichen Vorschriften, Vorgaben und Notwendigkeiten Rechnung getragen wird. Diese Vorschriften verlangen vor allem folgende Maßnahmen:

- Schriftliche Bestellung des schulischen Datenschutzbeauftragten und Vertreters (§ 5 Abs. 1 HDSG) und § 11 der Verordnung über die Verarbeitung personenbezogener Daten in Schulen und statistische Erhebungen an Schulen

- Erstellung, Fortführung und Umsetzung eines schriftlichen IT-Sicherheitskonzeptes nach § 10 Abs. 2 Satz 2 HDSG.

- Abstimmung notwendiger Maßnahmen im Rahmen der Äußeren Schulverwaltung mit dem Schulträger.

4. Technische und Organisatorische Maßnahmen

4.1 Sicherstellung ausreichender Qualifikation

Das Personal, das für den Betrieb und die Wartung der IT in den Schulen zuständig ist, muss die ihm zu übertragenden Aufgaben fachkundig erfüllen können. Beauftragt der Schulträger eigenes oder externes Personal, so trägt er unmittelbar die Verantwortung.

4.2 Räumliche Sicherung der IT-Anlagen

Räume mit Netzstrukturen und IT-Systemen, die den Zugang auf das Verwaltungsnetz der Schulen bzw. auf das kommunale Schulträgernetz bereitstellen, unterliegen besonderen Schutzmaßnahmen, da die entsprechenden Gebäude der Öffentlichkeit während der regulären Dienstzeiten und gegebenenfalls auch zu bestimmten Anlässen auch an Wochenenden (z. B. Schulfeste oder Schule als Wahllokal) oder an Wochentagen nach der regulären Hauptarbeitszeit (z. B. Elternabende, Infoveranstaltungen
etc.) zugänglich sind.

Es müssen Maßnahmen und Regelungen getroffen werden, um den unberechtigten Zutritt zu schutzbedürftigen Räumen zu verhindern:

- Zutrittskontrolle:
  Räume, in denen PCs oder Netzwerkkomponenten des Verwaltungsnetzes stehen, sollten mit einem geeigneten Schutz gegen unbefugten Zutritt und Einbruch etc. versehen sein. Ggf. ist dieser vom Schulträger einzufordern. Der Zutritt zu Räumen mit Netzstrukturen und IT-Systemen ist ausschließlich berechtigten Personen (Schulleitung, Lehrer, Verwaltungsangestellte, ggf. Netzwerkadministrator) gestattet. Die Räume müssen sicher verschließbar sein, der Kreis der zutrittsberechtigten Personen muss genau festgelegt werden (z. B. durch dokumentierte Schlüsselverwaltung) und die Kenntnisnahme der entsprechenden Regelungen durch die berechtigten Personen muss dokumentiert werden. Anderen Personen (z. B. Schülern etc.) ist der Zutritt allenfalls in Begleitung oder Anwesenheit berechtigter Personen erlaubt. Für Personenkreise, die außerhalb der regulären Öffnungszeiten die Räume betreten müssen (z. B. Reinigungspersonal o. ä.) können evt. in Absprache mit dem Schulträger Sondervereinbarung getroffen werden. Bei nicht besetzten Räumen, in denen Client-Systeme bzw. Netzinfrastruktur stehen, sind Fenster und Türen verschlossen zu halten. Schlüssel zu diesen Räumen sind nur an berechtigte Personen (kontrolliert bzw. dokumentiert) auszugeben und dürfen nicht an andere Personen weitergegeben werden. (Zugangs- und Zutrittsschutz)

- Benutzer- und Zugriffskontrolle:
  Für ein gesichertes Login an einem IT-System ist die entsprechende Authentifizierung, bestehend aus dem Benutzernamen und einem geheim zu haltenden Passwort notwendig. Regelungen zur Wahl eines sicheren Passworts sollten sich an der BSI Maßnahme M2.11 „Regelung des Passwortgebrauchs“ orientieren (Zugangs- und Zugriffsschutz). Das Passwort ist personenbezogen zu halten und in angemessenen Zeiträumen zu wechseln. Passwörter sollen mindestens acht Zeichen umfassen und möglichst eine komplexe Zusammensetzung aus Buchstaben (groß/klein), Sonderzeichen und Ziffern aufweisen. Passwörter dürfen in keinem Fall zugänglich notiert oder an andere Personen weitergegeben werden. Für Notfall-Passwörter gilt die Ausnahme, dass diese in einem Passwort-Safe hinterlegt werden dürfen.

5. Verwaltungsnetz und Verwaltungsrechner

Bei den kommenden Ausführungen wird vom (Schul-)Verwaltungsnetz und von Verwaltungsrechnern gesprochen. Verwaltungsrechner sind alle Computersysteme, die ausschließlich für Verwaltungszwecke zu nutzen sind. Eine gleichzeitige Nutzung zur Unterrichtsvorbereitung oder Ähnlichem ist nicht gestattet. Verwaltungsrechner sind entweder Stand-Alone-Geräte, die mit keinem anderen Rechner verbunden sind, sie können Geräte in einem lokalen Schulverwaltungsnetz sein und sie können darüber hinaus an das Hessische Schulverwaltungsnetz angebunden sein. In keinem Fall dürfen sie über einen ungeschützten Internetzugang verfügen. Daher bieten das Hessische Schulverwaltungsnetz bzw. die Schulnetze der Schulträger gesicherte Internetzugänge an.

Für diese Rechner gilt:

- Rechner, Datenträger und aktive Komponenten können nicht aus dem Unterrichtsbereich in den Verwaltungsbereich oder umgekehrt aus dem Verwaltungsbereich in den Unterrichtsbereich übernommen werden, ohne dass vorher vorhandene Software und Daten grundlegend gelöscht werden. Vorgehensweisen und Methoden werden im BSI Maßnahmenkatalog „M 2.167 Sicheres Löschen von Datenträgern“ beschrieben. Über das Löschen der Daten und Datenträger ist ein Vermerk zu den Akten zu nehmen.

- Entsprechend der Art des Einsatzes ist auf Schulverwaltungsrechnern auch nur solche Software einzusetzen, die zur Erfüllung dieser Aufgaben dient. Die Installation von nicht genehmigter Software (z. B. durch Downloads vom Internet oder von anderen Quellen) auf den Client-Rechnern ist nicht erlaubt und sollte nach Möglichkeit technisch unterbunden werden. (Schutz vor unbeabsichtigter Installation von Schadsoftware und störende bzw. beeinträchtigende Wechselwirkungen mit benötigter Software). Die Schulträger können Genehmigungsvorbehalte zur Installation von Software erlassen. Damit soll die Verträglichkeit der Software untereinander auf den Rechnern und insbesondere die aufgabengebundene Nutzung des PCs gesichert bleiben.

- Befinden sich die Client-Systeme der Verwaltung im Verwaltungsnetz in Räumen mit Publikumsverkehr (z. B. Sekretariat oder dergleichen) ist durch eine geeignete Aufstellung der Client-Systeme (einschließlich Tastatur, Bildschirm, Drucker, Scanner und dergleichen) der Zugriff von Unbefugten zum System und die Einsichtnahme von Daten zu verhindern. Bei Abwesenheit der Zugriffsberechtigten ist das Client-System entweder ganz auszuschalten oder zu sperren. In jedem Fall muss sich spätestens nach 10 Minuten „Ruhephase“ ein mit Passwortschutz ausgestatteter Bildschirmschoner aktivieren (Zugangs- und Zugriffsschutz).

- Die Konfiguration bzw. die vorhandenen Sicherheitseinstellungen der Client-Rechner dürfen durch die Benutzer nicht verändert werden. Dies sollte nach Möglichkeit technisch unterbunden werden. Dies betrifft Soft- und Hardware. Bei entsprechenden Fragestellungen oder Problemen ist der Schulleiter und ggf. der für die Schule zuständige Support zu kontaktieren. (Zugangs- und Zugriffsschutz)

6. Hardware

6.1 Schulische Netzwerke

In der Regel existieren in den Schulen Netzwerkverbindungen für Verwaltungszwecke (sog. Verwaltungsnetz) und für pädagogisch-didaktische Zwecke (sog. Pädagogisches Netzwerk). Diese beiden Netzwerke sind physikalisch oder logisch strikt voneinander getrennt zu halten, da ihr Schutzbedarf jeweils unterschiedlich ist und verschiedene Zugriffsberechtigungen vorliegen können. (Schutz vor unbefugtem Zugriff auf die Netzinfrastruktur, Systeme und dort verarbeitete Daten)

- Eine sichere logische Trennung der Netze (z. B. durch Nutzung von VLANs auf Switches) ist technisch möglich. Die Sicherheitskonzepte zur logischen Trennung sollten die im IT-Grundschutzhandbuch des BSI im Baustein 7.11 Router „und Switches“ vorgesehenen Maßnahmen berücksichtigen und müssen dem aktuellen Stand der Technik entsprechen.

- Auf den Einsatz von WLAN sollte aus Sicherheitsgründen verzichtet werden. (Schutz vor unbefugtem Zugriff auf die Netzinfrastruktur, Systeme und dort verarbeitete Daten). In besonders begründeten Ausnahmefällen kann der Einsatz von WLAN auf Basis eines entsprechenden Sicherheitskonzeptes erfolgen.

- Zentrale Netzwerktechnik wie Router, Switches und Hubs soll in gesicherten, nicht öffentlich zugänglichen Räumen oder Schutzschränken untergebracht werden (s. auch Vorgaben für die IT-Infrastruktur). (Zugangs und Zutrittsschutz)

- Lehrkräfte können nur im Einvernehmen mit dem Schulträger zur Wartung der Netzwerke herangezogen werden, Schüler in keinem Fall.

6.2 Nutzung privater IT-Geräte

Private IT-Geräte dürfen grundsätzlich nicht zur Erledigung schulischer Verwaltungsarbeit benutzt werden. Eine Ausnahme bildet die Nutzung von Rechnern am häuslichen Arbeitsplatz der Lehrkräfte (s. Verarbeitung personenbezogener Daten am häuslichen Arbeitsplatz der Lehrkraft, Erlass vom 21. August 2009 [ABl. S. 726], Az.: I.7 - 000.256.000-00027)

6.3 Mobile IT-Geräte

Mobile IT-Geräte, die in das Hessische Schulverwaltungsnetz eingebunden werden sollen, müssen ausschließlich dienstlich genutzt werden und dürfen in keiner Form anders als über das Schulverwaltungsnetz mit dem Internet verbunden werden.

6.4 Mobile Datenträger

Werden personenbezogene Daten auf mobile Datenträger ausgelagert, so ist mit entsprechender Sorgfalt zu verfahren.

- Der Datenträger mit personenbezogenen Daten ist zu registrieren.

- Soll der Datenträger auch außerhalb des Schulsekretariats bzw. der Büroräume der Schulleitung genutzt werden, so sind personenbezogene Daten zu verschlüsseln und ein gesicherter, überwachter Transport zu gewährleisten. Bei Daten die aus der LUSD geliefert werden (Externer Notenerfassungs-Client) wird diese Verschlüsselung automatisch hergestellt.

- Dienstlich gestellte Datenträger dürfen grundsätzlich nur für dienstliche Zwecke und zum Datentransport zwischen Verwaltungsrechnern verwendet werden.

- Werden die auf mobilen Datenträgern gespeicherten Daten nicht mehr benötigt bzw. sind sie in das zentrale System zurück zu spielen und auf dem mobilen Datenträger zu löschen. Die Schulen und Schulträger können für die Nutzung mobiler Datenträger Richtlinien erlassen oder eine spezielle Schutzsoftware zur technischen Registrierung von externen Datenträgern einsetzen. Andere, nicht registrierte Datenträger können dann an den Verwaltungsrechnern nur noch nach gesonderter Freigabe verwendet werden.

7. Schutz vor Schadprogrammen

In den dezentralen Netzen liegt die Verantwortung für einen funktionsfähigen und stets aktuellen Schutz vor Schadprogrammen beim Schulleiter und Schulträger gleichermaßen. Zu den Aufgaben der Schulleitung gehören unter anderem

- die Sensibilisierung der Nutzer für vorhandene Gefahren durch Viren

- die Information der Nutzer über Vorsichtsmaßnahmen und Verhaltensregeln zum Schutz vor Viren

- dafür zu sorgen, dass geeignete Virenschutzmaßnahmen auf gefährdeten IT-Systemen implementiert werden

- das Aufstellen von Verhaltensregeln für einen eingetretenen oder vermuteten Virenbefall, z. B. Benachrichtigung einer Hotline oder des IT-Supports, um eine Beseitigung der Virusinfektion zu veranlassen und sofortiges Einstellen der Arbeit am befallenen Client-Rechner

8. Konventionelle und elektronische Datenspeicherung und Datensicherung

8.1 Aufbewahrung von Schülerakten

Die Schülerakten, Karteikarten mit personenbezogenen Angaben, entsprechende Listen etc. sind grundsätzlich nur in ausreichend sicheren Schränken zu verwahren (Stahlschrank mit Sicherheitsschloss o. ä.). Bei größeren Schulsystemen empfiehlt es sich, die Akten stufen- oder zweigweise gegliedert in unterschiedlichen Schränken aufzubewahren, so dass dann, wenn ein Zugang notwendig wird, nie der gesamte Aktenbestand angeboten werden muss.

8.2 Elektronische Speicherung

Werden über die Nutzung der LUSD hinaus in der Schule elektronische Dokumente auf Verwaltungsrechnern gespeichert, so ist dafür – ggf. in Absprache mit dem Schulträger – ein entsprechendes Dateiablage-Konzept zu entwickeln. Handelt es sich um Dateien mit personenbezogenen Inhalten. muss der Zugang zu den entsprechenden Ablagesegmenten ausreichend geschützt werden, handelt es sich dabei auch um Daten nach § 7 Abs. 4 Hessisches Datenschutzgesetz, sind diese Daten zwingend verschlüsselt abzulegen.

8.3 Datensicherung

Zur Gewährleistung von Datenschutz und IT-Sicherheit gehört auch, dass die Verfügbarkeit der Daten gesichert ist. Für die Daten der LUSD übernimmt dies die Hessische Zentrale für Datenverarbeitung, dort ist ein entsprechendes Datensicherungssystem aktiv.

- Für darüber hinaus auf Verwaltungsrechnern/Servern der Schule gehaltene Daten hat die Schulleitung für eine entsprechende Datensicherung zu sorgen. Diese hat regelmäßig und in ausreichender Frequenz zu erfolgen (Tages-, Wochen- und Monatssicherung).

- Die Datenträger, auf denen diese Datensicherung erfolgt sind entsprechend der Sensibilität der jeweiligen Dateien geschützt aufzubewahren. Dies bedeutet nicht nur den Schutz vor unbefugten Zugriffen, sondern auch vor Beschädigung durch Feuer, Wasser oder Diebstahl. Daher sind sie nicht im gleichen Raum wie Rechner oder Server aufzubewahren, sondern in einem anderen Raum, möglichst in einem anderen Gebäude(teil)

- Existiert an der Schule ein Client-Server-System, so sind die Daten grundsätzlich auf dem Server zu speichern. Die Daten auf dem Server sind zentral zu sichern und die Datenträger vorzugsweise in separaten Räumlichkeiten zu verwahren. Zusätzliche lokale Speicherung personenbezogener Daten auf den Clients hat zu unterbleiben.

9. Elektronischer Mailverkehr

9.1 Postfächer

Mit der Einrichtung des Hessischen Schulnetzes erhielten alle beteiligten hessischen Schulen drei Funktionspostfächer:

- Das Funktionspostfach „Poststelle“

- Das Funktionspostfach „Schulleitung“

- Das Funktionspostfach „Landesaufgaben“

Darüber hinaus konnten personalisierte Postfächer zur Verfügung gestellt werden. In einzelnen Schulträgerbereichen mit eigenen Netzen werden schulträgerspezifische Postfächer genutzt, die ebenfalls an das Schulverwaltungsnetz angebunden sind.

Das Funktionspostfach „Poststelle“ ist als offizielle Mailadresse der Schule zu verwenden. Es fungiert zugleich als elektronische Posteingangsstelle.

Die Verwendung der anderen Funktionspostfächer ergibt sich aus ihrer Bezeichnung.

Eine Vertretungsregelung hat sicher zu stellen, dass eingehende Mail geöffnet und bearbeitet werden kann. Dies kann erfolgen durch Weiterleitung der Posteingänge oder durch Zugriffsgewährung auf das E-Mail-Postfach.

Achtung:

Von den im Schulnetz eingerichteten Postfächern darf keine automatisierte Weiterleitung der Mails an private Postfächer außerhalb des Schulverwaltungsnetzes erfolgen. (vgl. dazu Abschnitt **Mail-Umleitung**)

9.2 Allgemeine Grundsätze der Nutzung
Die dienstliche Mailadresse ist nur für dienstliche Zwecke zu nutzen.

Grundsätzlich sollen im innerbehördlichen Schriftverkehr alle Schreiben und sonstige Dokumente per E-Mail versandt werden, die nicht eine persönliche Unterschrift erfordern oder vertraulich zu behandelnde Daten enthalten.

9.3 Mail-Eingang
Die elektronischen Informationen (Mails) sind in geeigneter Weise in den Geschäftsgang zu bringen und, soweit sie für den Nachweis des Standes und der Entwicklung der Vorgangsbearbeitung nicht offenkundig unerheblich sind, elektronisch oder in Papierform (als Ausdruck) zu den Akten zu nehmen. (siehe „Archivierung“)

9.4 Mail-Ausgang
Bei der Nutzung der E-Mail ist zunächst zu unterscheiden, ob es sich um allgemeine Nachrichten, Terminabsprachen o.ä. handelt oder ob ein Dokument mit Aktenrelevanz versandt werden soll. Die folgenden Regelungen beziehen sich auf die letztgenannten Dokumente.

Der elektronische Versand in Form einer einfachen E-Mail (unverschlüsselt und unsigniert) eignet sich nicht, soweit höherwertige Formvorschriften (z. B. handschriftliche Unterschrift, Urkundenform) bestehen. Für einen Versand per E-Mail sind die einschlägigen gesetzlichen Bestimmungen zum Ersatz dieser Formen in elektronischen Dokumenten zu beachten.

Werden keine Verschlüsselungsverfahren angewendet und erfolgt der Versand nicht oder nicht ausschließlich im Schulnetz, sondern im Internet, entsprechen E-Mails einer „offenen“ Postkarte“. Die Übermittlung von vertraulich zu behandelnder Informationen oder schutzwürdiger personenbezogenen Daten darf daher auf elektronischem Weg nur bei Nutzung einer den BSI-Standards entsprechenden Verschlüsselung erfolgen.

Im elektronischen Dokument genügt an Stelle der Unterschrift der Vermerk „gez.“ in Verbindung mit dem Namen der unterzeichnenden Person und der Fixierung des Datums. Ein Bestätigungsvermerk entfällt. Ausgehenden E-Mails, die auch in Papierform vorhanden sind, liegt ein abgezeichneter Entwurf zu Grunde. Der Versand ist durch handschriftlichen Vermerk oder Versandprotokoll aktenkundig zu machen.

9.5 Mail-Umleitung
Eine Umleitung von Mails auf Postfächer im Internet birgt immer die Gefahr, dass Mails von nicht berechtigten Personen gelesen und auch verändert werden können.
Daher gilt:

- Für das Postfach „Landesaufgaben“ ist keine Form der Umleitung zulässig.

- Eine automatisierte Umleitung darf im Übrigen nur auf solche Postfächer eingerichtet werden, die sich im Schulnetz oder einem entsprechend abgesicherten Netz des Schulträgers befinden.

- Eine automatisierte Umleitung in das sichere Netz des Schulträgers erfordert die Zustimmung und Absprache zwischen Schulträger und HKM.

- Eine manuelle Umleitung auf Postfächer im Internet ist nur im Einzelfall zulässig und auch nur dann, wenn geprüft wurde, dass die Mail keine vertraulichen oder personenbezogenen Daten enthält.

Es ist grundsätzlich zu beachten, dass bei umgeleiteten Mails und der Nutzung der „Antworten-Funktion“ als Absenderangabe nicht mehr die offizielle Schuladresse erscheint.

9.6 Archivierung

Da die Kapazitäten der Postfächer beschränkt sind, sind diese immer wieder rechtzeitig zu sichten. Aktenrelevante Mails sind als Ausdruck den Akten beizufügen, oder –wenn ein elektronisches Dokumentenmanagementsystem vorhanden ist – dort abzuspeichern und zu archivieren. Das Mailsystem ersetzt keine Ablage. Danach sind die Mails zu löschen.

Die übrige Post ist nach angemessener Frist zu löschen.

9.7 Geschützte Dokumente und Anlagen

Es ist notwendig, Dokumente, die man vor Veränderungen schützen will, im PDF-Format zu versenden. Dieses Format erfordert in der Regel auch weniger Speicherplatz.

Versendet man mit der Mail Dokumente als Anhang, so ist auf deren Größe zu achten, vor allem, wenn ein großer Adressatenkreis erreicht werden soll. Ausführbare Dateien (Endungen wie exe oder mdb) werden vom System aus Sicherheitsgründen gesperrt.

10. Erhebung und Veröffentlichung von Daten:

Für die Erhebung von nicht personenbezogenen Daten im Zuständigkeitsbereich des Hessischen Kultusministeriums wird vorzugsweise das Verfahren ESDAL (**E**rhebung **S**tatistischer **DA**ten im **L**andesschulnetz) eingesetzt. Das Verfahren bietet die Vorteile einer einfachen Bedienung über eine Browser-Oberfläche, einer sicheren Datenübermittlung aus dem Landesschulnetz in das Landesverwaltungsnetz und der Nutzung der vorhandenen Benutzerkonten des Verfahrens LUSD. Eine gesonderte Benutzerkontenverwaltung für die Schulen, wie sie bei der Erhebung von Daten über das Internet üblicherweise erforderlich ist, kann somit entfallen. Es entfällt ebenfalls der Versand von Dateien mit Erfassungsdaten als E-Mail-Anhang, womit die Zuverlässigkeit und Sicherheit der Datenübermittlung verbessert wird.

Die Publikation von Statistischen Berichten aus dem Landesverwaltungsnetz in das Landesschulnetz erfolgt vorzugsweise über das Verfahren ISIS (**I**nformations **S**ystem **I**m **S**chulnetz). Das Verfahren erlaubt die schulbezogene Veröffentlichung von Berichten in unterschiedlichen technischen Formaten im Landesschulnetz. Über die Nutzung des Berechtigungssystems der LUSD wird sichergestellt, dass Zugriff auf den Bericht über eine Schule nur die jeweilige Schule und das Aufsichtführende Staatliche Schulamt haben.

11. Aufhebung von Erlassen

Die Richtlinie zur Nutzung des Hessischen Schulnetzes und zum Umgang mit E-Mail, Erlass vom 8. August 2007 (ABl. S. 559), Az.: I.7 – 640.000.010-46- wird aufgehoben