

Einwilligungserklärung (Digitale Schule)

Hiermit bestätige ich,

Vorname, Name: _____ Klasse: _____

dass ich die Texte (<https://gymall.de/privacy.pdf> [Stand 22.09.2021]) über das Reglement zur digitalen Arbeit an unserer Schule

- Nutzungs- Einwilligungserklärung IServ (S. 1-3) ¹
- Information und Einwilligungserklärung Videokonferenzen (S. 4-6) ²
- Nutzerordnung für das IServ-Videokonferenztool (S. 7-10) ³
- Regelungen zu Videokonferenzen (S. 11-12) ⁴
- Nutzungsbedingungen Moodle (S. 13-17) ⁵
- Nutzungsregelungen für WLAN-Zugang und Internet-Nutzung (S. 18-19) ⁶

gelesen und zur Kenntnis genommen habe sowie mich damit einverstanden erkläre.

(Datum)

(Unterschrift Schüler:in⁷)

(Datum)

(Unterschrift Sorgeberechtigte*r)

¹ Quelle: <https://iserv.de/downloads/privacy/>

² Quelle: <https://iserv.de/downloads/privacy/>

³ Quelle: <https://iserv.de/downloads/privacy/>

⁴ Quelle: <https://iserv.de/downloads/privacy/>

⁵ Quelle: <https://moodle-ola.de/moodle-datenschutz.html>

⁶ Quelle: <https://iserv.de/downloads/privacy/>

⁷ Ab 14 Jahren ist eine Unterschrift der Schüler:in notwendig.

Gymnasium Allermöhe

Präambel

Die Schule stellt ihren Schülerinnen, Schülern und Lehrkräften und anderen Mitarbeitern (im Folgenden: Nutzer) als Kommunikations- und Austauschplattform IServ zur Verfügung. IServ dient ausschließlich der schulischen Kommunikation und ermöglicht allen Nutzern, schulbezogene Daten zu speichern und auszutauschen. Alle Nutzer verpflichten sich, die Rechte anderer Personen zu achten.

Nutzungsmöglichkeiten

Die Schule entscheidet darüber, welche Module von IServ für den innerschulischen Gebrauch freigeschaltet werden und welcher Nutzerkreis zu diesen Zugang erhält. Um IServ nutzen zu können, ist eine Einwilligung des Nutzers notwendig.

Allgemeine Verhaltensregeln

Jeder Nutzer erhält ein Nutzerkonto. Das Nutzerkonto muss durch ein nicht zu erratendes Passwort von mindestens acht Zeichen Länge (Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen) gesichert werden. Es ist untersagt, das Passwort anderen Nutzern mitzuteilen. Erfährt ein Nutzer, dass jemand unberechtigt Kenntnis von seinem Passwort hat, so muss er sein Passwort unverzüglich ändern.

Sollte ein Nutzer sein Passwort vergessen haben, ist er verpflichtet, das durch einen Admin-istrator neu vergebene Passwort beim nächsten Einloggen sofort zu ändern. Nur der Nutzer selbst darf ein neues Passwort für sich bei einem Administrator beantragen.

Alle Nutzer sind verpflichtet, eingesetzte Filter und Sperren zu respektieren und diese nicht zu umgehen.

Die Sicherung eigener in IServ gespeicherter Dateien gegen Verlust obliegt der Verantwortung der Nutzer, da eine Rücksicherung mit unverhältnismäßigem Aufwand verbunden wäre.

Das Senden, Aufrufen und Speichern jugendgefährdender und anderer strafrechtlich relevanter Inhalte ist auf dem Schulserver ebenso verboten wie die Speicherung von URLs (Webseiten) oder Links auf jugendgefährdende Websites oder Websites mit strafrechtlich relevanten Inhalten. Die Schule übernimmt keine Verantwortung für die Inhalte und die Art gespeicherter Daten. Weil umfangreiche Up- und Downloads die Arbeitsgeschwindigkeit des Servers beeinträchtigen, sind diese nicht erlaubt. Die Installation oder Nutzung fremder

Software darf und kann nur von den Administratoren durchgeführt werden. Ausnahmen sind vorab mit den Administratoren abzusprechen.

Administratoren

Die Administratoren haben weitergehende Rechte, verwenden diese aber grundsätzlich nicht dazu, sich Zugang zu persönlichen Konten bzw. persönlichen Daten zu verschaffen. Dies ist durch eine schriftliche Vereinbarung zu regeln.

Protokolle

Das IServ-System erstellt Log-Dateien (Protokolle), die in schwerwiegenden Fällen (z. B. bei Regelverstößen, Betrugs- und Täuschungsversuchen oder Rechtsverstößen) auf Weisung der Schule ausgewertet werden können.

Hausaufgaben

Hausaufgaben können über IServ gestellt werden, müssen aber im Unterricht angekündigt werden. Die Lehrkräfte achten dabei auf einen angemessenen Bearbeitungszeitraum.

Verhaltensregeln zu einzelnen IServ-Modulen⁸

E-Mail

Soweit die Schule den Nutzern einen persönlichen E-Mail-Account zur Verfügung stellt, darf dieser nur für die interne schulische Kommunikation verwendet werden. Die Schule ist kein Anbieter von Telekommunikation im Sinne von § 3 Nr. 6 Telekommunikationsgesetz. Ein Rechtsanspruch der Nutzer auf den Schutz der Kommunikationsdaten im Netz besteht gegenüber der Schule somit grundsätzlich nicht. Die Inhalte der Mails und welche personenbezogenen Daten in IServ verarbeitet werden dürfen, müssen sich an den für unser Bundesland geltenden Schulgesetz orientieren.

Die Schule ist berechtigt, im Falle von konkreten Verdachtsmomenten von missbräuchlicher oder strafrechtlich relevanter Nutzung des E-Mail-Dienstes die Inhalte von E-Mails zur Kenntnis zu nehmen. Die betroffenen Nutzer werden hierüber unverzüglich informiert.

Der massenhafte Versand von E-Mails, sowie E-Mails, die dazu gedacht sind, andere Nutzer über Absender oder Glaubhaftigkeit der übermittelten Nachricht zu täuschen, ist verboten.

Forum

Soweit die Schule eine Forum-Funktion zur Verfügung stellt, gelten dieselben Vorgaben wie bei der E-Mail-Nutzung. Neben schul-öffentlichen Foren stehen auch Foren mit eingeschränktem Nutzerkreis zur Verfügung, z.B. Gruppenforen. Darüber hinaus sind die

⁸ Informationen zu den von der Schule eingesetzten Modulen und den dort verarbeiteten Daten finden Sie im Detail in dem Dokument „Welche Daten werden in welchem Modul verarbeitet.docx“, das Ihnen die Schule gern übergibt. Sie finden es auch unter <https://www.iserv.de/downloads/privacy/> im Dokumentenpaket für Schulen.

Moderatoren der Foren berechtigt, unangemessene Beiträge zu löschen oder zu bearbeiten. Moderatoren dürfen nur in dem ihnen anvertrauten Foren moderieren.

Kalender

Kalendereinträge für Gruppen werden nach bestem Wissen eingetragen und nicht manipuliert.

Messenger

Soweit die Schule die Messenger-Funktion zur Verfügung stellt, gelten dieselben Vorgaben wie bei der E-Mail-Nutzung.

Videokonferenzen

Sofern die Schule das Modul einsetzt, werden die Nutzer mit einer separaten Nutzungsordnung über das Verfahren informiert. Auch eine eigene Einwilligung ist dann notwendig.

Verstöße

Im Fall von Verstößen gegen die Nutzungsordnung kann das Konto temporär oder permanent gesperrt werden. Damit ist die Nutzung schulischer Computer sowie die Nutzung von IServ auf schulischen und privaten Geräten nicht mehr möglich.

Unabhängig davon besteht die Möglichkeit, Nutzern den Zugang zu einzelnen Komponenten oder Modulen zu verweigern, sodass beispielsweise das Anmelden am Schul-WLAN nicht mehr möglich ist, aber auf Schul-Computern und Zuhause IServ weiterhin genutzt werden kann.

Die Ahndung von Verstößen liegt im Ermessen der Administratoren.

Datenschutzrechtliche Information (Art. 12 DSGVO) zum IServ-Videokonferenztool

Auf dieser Seite informieren wir Sie aufgrund Art. 12 DSGVO über die zur Nutzung des IServ Videokonferenztools erforderliche Verarbeitung von personenbezogenen Daten.

Wer ist verantwortlich für die Verarbeitung der Daten meines Kindes?

Verantwortlich ist die Schule: [Gymnasium Allermöhe, Walter-Rothenburg-Weg 41, 21035 Hamburg; Schulleitung: Olaf Colditz]

An wen kann ich mich wenden, wenn ich Fragen zum Datenschutz habe?

Fragen zum Datenschutz können Sie an den behördlich bestellten schulischen Datenschutzbeauftragten stellen: [Olaf Colditz, olaf.colditz@bsb.hamburg.de]

Zu welchem Zweck sollen die Daten meines Kindes verarbeitet werden?

Das IServ Videokonferenztool ermöglicht Unterricht und Besprechungen, bei denen Beteiligte nicht zusammen in einem physikalischen Raum sind. Durchführung von Online-Unterrichtseinheiten in der Lerngruppe und individueller Betreuung und Beratung in Kleingruppen oder Einzeltreffen zwischen Schüler und Lehrkraft sind dadurch möglich. Zudem werden die Schüler so datenschutzkonform an das Medium und die Möglichkeiten herangeführt, die heutzutage nicht mehr wegzudenken sind.

Auf welcher Rechtsgrundlage erfolgt die Verarbeitung?

Die Verarbeitung erfolgt auf der Grundlage Ihrer Einwilligung, da IServ kein durch die Behörden genehmigtes Lehrmittel ist, ist nur diese Möglichkeit gegeben.

Welche personenbezogenen Daten meines Kindes werden bei Teilnahme an einer IServ Videokonferenz verarbeitet?

Videokonferenzen in der Schule finden in der Regel in einer Gruppe von Teilnehmern mit IServ-Account statt.

Bei der Teilnahme an einer Videokonferenz) werden neben Bild- und Tondaten zusätzliche Daten zur Konferenz verarbeitet: Name des Raumes, IP Nummer des Teilnehmers und Informationen zum genutzten Endgerät. Je nach Nutzung der Funktionen in einer Videokonferenz fallen personenbezogenen Inhalte von Chats, gesetztem Status, Eingaben bei Umfragen, Beiträge zum geteilten Whiteboard, durch Upload geteilte Dateien und Inhalte von

Bildschirmfreigaben an. Eine Speicherung von Videokonferenzen und den genannten Daten durch die Schule oder IServ erfolgt nicht. Es muss zum Videokonferenztool eine Nutzerordnung und Hinweise geben, da ja der Kontakt oft aus dem häuslichen Bereich der Teilnehmer erfolgt und besonders dort Daten geschützt werden sollten. Aufnahmen sind generell zu untersagen.

Wer hat Zugriff auf die personenbezogenen Daten meines Kindes?

Alle Teilnehmer einer Videokonferenz können dort Daten durch Sehen, Hören und Lesen verarbeiten. Der Präsentator hat zusätzlich die Auswertungen zu Umfragen zur Verfügung. IServ selbst hat nur Zugriff auf die Daten im Rahmen der Auftragsverarbeitung also nur auf Weisung der Schule.

An wen werden die Daten meines Kindes übermittelt und wie lange werden diese Daten gespeichert?

Unsere Videokonferenz-Instanz wird von IServ für uns betrieben. IServ verarbeitet die personenbezogenen Daten Ihres Kindes ausschließlich in unserem Auftrag. Demnach darf IServ sie nur entsprechend unserer Weisungen und für unsere Zwecke und nicht für eigene Zwecke nutzen. Es werden also keine Daten an Dritte weitergegeben. Die Daten werden bei IServ nicht gespeichert.

Die Schule speichert ebenso keine personenbezogenen Daten. Videokonferenzen und Chats werden generell nicht aufgezeichnet. Die Inhalte von Chats, geteilte Dateien und Whiteboards werden in der Plattform gelöscht, sobald ein Konferenzraum geschlossen wird. Ausnahmen müssen extra in der Schule vereinbart werden.

An die Server der IServ GmbH werden Klarnamen der Teilnehmer, IP-Adressen, Browserkennungen, Berechtigungen, Videokonferenz-Raum-Einstellungen, Raumname und die IP-Adresse sowie eine eindeutige Identifikationsnummer des IServs übermittelt. Auf dem Videokonferenz-Server haben die Benutzer die Möglichkeit, Daten in Form von Beteiligungen am virtuellen Whiteboard, Chat-Nachrichten, hochgeladenen Präsentationen und Notizen einzugeben. Außerdem fallen Metadaten wie Dauer der Videokonferenz und Zeitstempel zu Ereignissen wie dem Beitritt oder dem Verlassen einer Konferenz an. Diese Daten werden frühestens zum Ende der Videokonferenz und spätestens nach Ablauf von sieben Tagen gelöscht. Sicherungskopien dieser Daten werden nicht angelegt.

Technische Information: Nehmen zu viele mit aktivierter Kamera an einer Videokonferenz teil, kann es zu Stabilitätsproblemen kommen Neben der eigenen Bandbreite ist die Qualität der Konferenz auch von dem eigenen Netzwerk abhängig. Verwenden Sie möglichst eine Kabelverbindung zum Router und vermeiden Sie WLAN.

Es ist Teilnehmern untersagt, Videokonferenzen mitzuschneiden. Die Verwendung von Software, die den Bildschirminhalt oder die Videokonferenzen aufnimmt, stellt einen Verstoß

gegen die DSGVO und das Recht am eigenen Bild dar. Ausnahmen müssen durch die Schulleitung genehmigt sein.

Einwilligung

Sehr geehrte Erziehungsberechtigte,

Wir legen großen Wert auf den persönlichen Kontakt zu unseren Schülerinnen und Schülern. Dazu möchten wir eine Videokonferenz- Plattform nutzen, um Sitzungen innerhalb der Lerngruppen unter Leitung einer Lehrkraft abzuhalten, und für Ihr Kind Beratung und Unterstützung durch Lehrkräfte in Kleingruppen und im Vier-Augen-Gespräch auch außerhalb des Schulgebäudes zu ermöglichen. Nutzen werden wir dazu das IServ Videokonferenztool, eine Plattform, die in Deutschland von vielen Schulen und Universitäten genutzt wird. Sie kann über Computer, Smartphone und Tablet genutzt werden.

Die Teilnahme an einer Videokonferenz erfordert nur das IServ-Nutzerkonto. Alle Inhalte der Videokonferenzen und begleitenden Chats bleiben im Kreis der Teilnehmer. Es erfolgt keine Aufzeichnung oder Speicherung durch die Schule oder den Anbieter. Schüler sind gehalten, bei einer Videokonferenz darauf zu achten, dass die Privatsphäre ihrer Familienmitglieder gewahrt bleibt. Bei Verstößen gegen diese Regel behält die Schule sich vor, Ihr Kind von Videokonferenzen auszuschließen bzw. die Teilnahme auf Audio zu beschränken.

Hierzu möchten wir hier Ihre Einwilligung einholen.



(Julian Lee)



(Thies Henken)



(O. Colditz Schulleiter)

Diese Einwilligung kann für die Zukunft jederzeit formlos bei der Schule widerrufen werden. Im Falle des (Teil-)Widerrufs wird Ihr Kind nicht oder nur über Ton an Videokonferenzen teilnehmen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit, der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Soweit die Einwilligung nicht widerrufen wird, gilt sie für die Dauer der Beschulung.

Gegenüber der Schule besteht ein Recht auf Auskunft über Ihre personenbezogenen Daten, ferner haben Sie ein Recht auf Berichtigung, Löschung oder Einschränkung, ein Widerspruchsrecht gegen die Verarbeitung und ein Recht auf Datenübertragbarkeit. Zudem steht Ihnen ein Beschwerderecht bei der Datenschutzaufsichtsbehörde unseres Bundeslandes zu.

Nutzungsordnung IServ Videokonferenzmodul

Inhalt

Inhalt	7
1 Rahmenbedingungen	7
2 Webkonferenzen	7
2.1 Zugangsdaten	7
2.2 Daten, die im Rahmen einer Webkonferenz gespeichert werden	7
2.3 Datenlöschung	8
2.4 Webkonferenz: Lehrer ☒ Schüler/in	8
2.5 Webkonferenz (Schulleitung ☒ Lehrerkräfte; Lehrerkräfte ☒ Lehrkräfte;	8
Schulleitungen ☒ Lehramtsanwärter/Lehrkräfte)	8
2.6 Webkonferenz (Lehramtsanwärter ☒ Lehramtsanwärter)	8
3 Regeln für Webkonferenzen und Fernunterricht	9
4 Empfehlungen für die Kommunikations- und Verhaltensregeln während	9
Webkonferenzen	9

Rahmenbedingungen

Über das Videokonferenzmodul können Webkonferenzräume in datenschutzkonformen Umgebungen zur Durchführung von synchronen Phasen des Fernlernens in Gruppen sowie zur individuellen Betreuung mit einem abgestuften Rollen- und Rechtemanagement eingerichtet und genutzt werden.

Webkonferenzen

Zugangsdaten

- An einer Webkonferenz dürfen nur berechtigte Personen teilnehmen.
- An einer Webkonferenz müssen sich die Teilnehmer mit einem persönlichen Account mit sicherem Passwort bzw. einen zeitlich befristeten, passwortgeschützten Link (Raum Sharing) anmelden.

Daten, die im Rahmen einer Webkonferenz gespeichert werden

Bei der Teilnahme an einer Videokonferenz werden folgende Daten verarbeitet:

- Nachname, Vorname
- Bild- und Audiodaten
- Name des Raumes
- IP-Nummer des Teilnehmers und Informationen zum genutzten Endgerät.

- Je nach Nutzung der Funktionen in einer Videokonferenz fallen Inhalte von Chats, gesetzter Status, Beiträge zum geteilten Whiteboard, Eingaben bei Umfragen, durch Upload geteilte Dateien und Inhalte von Bildschirmfreigaben an.

Die Aufzeichnung von Videokonferenzen ist deaktiviert.

Datenlöschung

Es werden keine personenbezogenen Daten im Zusammenhang mit der Nutzung des IServ Videokonferenz-Moduls dauerhaft gespeichert. Videokonferenzen werden nicht aufgezeichnet. Die Inhalte von Chats, Notizen, geteilte Dateien und Whiteboards werden gelöscht, sobald ein Konferenzraum geschlossen wird.

Webkonferenz: Lehrer & Schüler/in

Wird die Nutzung des Moduls von der Schule als notwendig angesehen, benötigt man keine Einwilligung der Schülerin / des Schülers bzw. der Erziehungsberechtigten.

Hinweis: Die Schülerin / der Schüler hat ein Widerspruchsrecht nach Art. 21 DSGVO, über das er in der Nutzungsordnung zu informieren ist. Die Schülerin / der Schüler ist dann auf anderen Wegen auf dem Laufenden zu halten.

Webkonferenz (Schulleitung & Lehrerkräfte; Lehrerkräfte & Lehrkräfte; Schulleitungen & Lehramtsanwärter/Lehrkräfte)

Eine Webkonferenz kann durchgeführt werden sofern sie

- *dienstlich erforderlich ist* (Konferenzen, Abteilungskonferenzen).
- Bei besonders sensiblen Meetings/Gesprächen (bspw. Einstellungsgesprächen, Beratungsgesprächen, ...) ist die Leitung des Meetings in besonderer Verantwortung die Teilnahme zu schützen bzw. zu begrenzen. Geeignete Maßnahmen, wie z.B. ein Passwort-Schutz, Warteraum mit Teilnahmezulassung, akustische und optische Verifizierung der Teilnehmenden sind unabdingbar.
- Fortführungen von sensiblen Meetings/Gesprächen – nachdem eine teilnehmende Person das Meeting scheinbar verlassen hat -, sind in dem Bewusstsein zu führen, dass die optische nicht mehr anwesende Teilnehmende eventuell weiterhin/noch im Meeting ist. Es ist ggf. in der alleinigen Verantwortung der Organisatoren das laufende Meeting ggf. zu beenden und z.B. ein neues Meeting zu starten, um vertrauliche Gespräche zu führen.

Webkonferenz (Lehramtsanwärter & Lehramtsanwärter)

Eine Webkonferenz kann durchgeführt werden sofern die beteiligten Personen zustimmen

Regeln für Webkonferenzen und Fernunterricht

- Bei Webkonferenzen und im Fernunterricht dürfen mittels IServ Videokonferenz-Modul keine Daten nach Art. 9 Datenschutzgrundverordnung (Gesundheitsdaten, personenbezogene Daten aus denen rassistische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder Gewerkschaftszugehörigkeit sowie Daten zum Sexualleben oder der sexuellen Orientierung hervorgehen) verarbeitet werden.
- Es ist grundsätzlich verboten, Gespräche und Übertragungen mitzuschneiden, aufzuzeichnen, zu speichern auch mit jeder Art auch mit Drittsoftware oder bspw. Handycams ..., außer dass die Lehrkraft dies erlaubt.
- Es ist generell untersagt, dass ein Dritter (auch Eltern, Freunde Geschwister usw.) beim Fernunterricht zuhören zusehen oder sonst wie einen Einblick in die Kommunikation erhalten.
- Der persönliche Account für den Zugang zur Webkonferenz bzw. zum Fernunterricht darf an keine andere Person weitergegeben werden.
- Keine Nutzung in öffentlich zugänglichen Räumen wie z.B. Cafés, Kneipen, Restaurants, ÖPNV, Warteräume, Arztpraxen, Läden usw.

Hinweis: Wählen Sie einen passenden Ort für die Videokonferenz, wenn Bild- und

Tonübermittlung aktiviert sind, da die anderen Konferenzteilnehmerinnen und -teilnehmer ihr privates Umfeld im Hintergrund sehen können. Ideal ist eine aufgeräumte Arbeitsumgebung mit unaufgeregtem Hintergrund oder eine weiße Wand. Kommunizieren Sie diesen Sachverhalt rechtzeitig vor der Konferenz auch an die Teilnehmenden.

Empfehlungen für die Kommunikations- und Verhaltensregeln während Webkonferenzen

- Die goldene Regel vorneweg: Wer nicht spricht, schaltet sein Mikrofon stumm! Headsets sind zwar für die Tonqualität empfehlenswert, jedoch übertragen sie auch Atem- und Schluckgeräusche besonders deutlich.
- Seien Sie sich bewusst, dass eine Kamera auf Sie gerichtet ist. Zeigen Sie eine freundliche, offene Körperhaltung und Körpersprache. Lächeln Sie!
- Schauen Sie so oft wie möglich in die Kamera. Ihre Konferenzpartner werden dies als direkte Ansprache wahrnehmen. Unter Umständen ist es hilfreich, einen Klebepunkt knapp neben der Kameralinse zu befestigen, den man mit den Augen fokussieren kann.
- Schalten Sie – wenn möglich – ihr eigenes Kamerabild klein. Die Verlockung sich selbst zu beobachten ist groß und lenkt Sie ab.

- Ändern Sie möglichst wenig an der Positionierung aus Ausrichtung der Kamera, nachdem die Konferenz begonnen hat. Nachjustierungen wirken auf die Konferenzteilnehmerinnen und –teilnehmer störend.
- Auch wenn die Webkonferenz am Computer stattfindet, vermeiden Sie „Nebenbeschäftigungen“ wie Tippen auf der Tastatur oder Herumklicken in verschiedenen Fenstern – vor allem bei aktiviertem Mikrofon. Wenn Ihr Betriebssystem einen Nicht-Stören-Modus hat, schalten Sie ihn ein.
- Nutzen Sie auch den Chat nicht für Nebengespräche. Die Chats sind für Fragen und Hilfen geeignet. Schalten Sie als Lehrkraft ggf. die privaten Chats von Teilnehmerinnen und Teilnehmer ab.
- Setzen Sie klare verbale Signale für Redebeginn und Redeende. Sprechen Sie etwas langsamer und deutlicher als in der direkten Kommunikation.
- Warten Sie – z.B. nach direkten Fragen – länger auf die Reaktion von Teilnehmerinnen und Teilnehmern als bei direkten Gesprächen im „echten Leben“.
- Nutzen Sie Gestik bewusst auch für affirmative Signale beim Zuhören, wie z.B. ein deutliches Nicken oder ein Daumen-nach-oben-Zeichen.
- Bei größeren Online-Seminaren: Lassen Sie sich bei Moderationsaufgaben unterstützen um sich selbst auch besser auf die Kommunikation mit den Teilnehmerinnen und Teilnehmern konzentrieren zu können. Bestimmen Sie beispielsweise einen Moderator der die Statusicons und den Chat im Blick behält und Ihnen Wortmeldungen und Fragen zum passenden Zeitpunkt weitergibt.

Regelungen zu Videokonferenzen

Videokonferenzen im Unterricht: Hinweise für die Schulgemeinschaft

Eine neue Vorschrift im Hamburgischen Schulgesetz regelt den Einsatz von Videokonferenzen im Unterricht an Hamburger Schulen. Dieser neue § 98c wurde in das Schulgesetz eingefügt, weil in der gegenwärtigen Corona-Pandemie zeitweise der Schulbetrieb auf Distanz- und Wechsel-/Hybridunterricht umgestellt werden musste. Das Schulgesetz setzt den Unterricht in Videokonferenzen mit dem regulären Unterricht gleich. Das heißt es gilt auch im Unterricht über Videokonferenzen Anwesenheitspflicht. Dadurch wird zudem die Bewertung der Mitarbeit in Videokonferenzen ermöglicht.

Videokonferenzsysteme lassen sich vielfältig im Distanz- und Wechsel-/Hybridunterricht sowie im regulären Unterricht im Klassenzimmer einsetzen. Die Schulbehörde hat zu diesem Zweck einen Orientierungsrahmen für schulische Videokommunikation erarbeitet und den Schulen zur Verfügung gestellt.

Der erfolgreiche Einsatz von Videokonferenzen in der Schule erfordert einen rücksichtsvollen Umgang miteinander – wie bei anderen Themen in der Schule auch. Diese Hinweise sollen die Eltern, Schülerinnen und Schüler sowie weitere Angehörige der Schulgemeinschaft über den verantwortungsvollen Gebrauch dieser digitalen Konferenzen informieren.

Videokonferenzsoftware

Schulen nutzen grundsätzlich für Videokonferenzen und Videoübertragungen im Rahmen des Unterrichts die Software BigBlueButton. Diese Software steht z.B. in den Systemen „LMS Lernen Hamburg“ und „IServ“ zur Verfügung. Bei Ausfällen und bedeutsamen Funktionsstörungen kann eine Schule andere Softwarelösungen dafür nutzen. Dann trägt die Schule dafür Sorge, dass der Datenschutz gewährleistet ist und wird ggf. gesondert darüber informieren.

Respektvoller Umgang und Netiquette

Alles, was im Präsenzunterricht zum guten Ton gehört, gilt genauso im Online-Unterricht per Videokonferenz. Die Klassenregeln gelten weiter. Für Videokonferenzen ist es darüber hinaus sinnvoll, sich innerhalb der Klasse oder Schulgemeinschaft auf eine „Netiquette“ oder Regeln für digitale Kommunikation zu verständigen. Das heißt, dass alle Teilnehmenden ganz besonders auf den respektvollen Umgang miteinander achten und die Privatsphäre aller Beteiligten beachten. Bei der Übertragung von Zuhause sollten nur wirkliche nötige Informationen per Bild preisgegeben werden. Die Kamerafunktion muss immer dann aktiviert werden, wenn es pädagogische Gründe erfordern. Die Lehrkraft beachtet neben den Persönlichkeitsrechten auch die persönlichen Lebensumstände der Schülerinnen und Schüler.

Vertraulichkeit und Verbot von Aufzeichnungen

Der Videounterricht ist streng vertraulich und nicht öffentlich. Ohne ausdrückliche Erlaubnis darf niemand Inhalte aus dem Unterricht weitergeben.

An Videokonferenzen dürfen nur Personen teilnehmen, die über individuelle Zugangsdaten Zutritt zum virtuellen Raum erhalten. Externe Personen dürfen nur eingeladen werden, wenn die Lehrkraft dies ausdrücklich erlaubt.

Es ist verboten, Ton- und Videoaufnahmen zu machen.

Unerlaubte Ton- und Videoaufnahmen stellen eine schwere Verletzung der Persönlichkeitsrechte dar. Nach § 49 des Hamburgischen Schulgesetzes ist ein solches Fehlverhalten eine Störung des Schulfriedens und kann weitreichende rechtliche Konsequenzen zur Folge haben. Darauf weisen die Lehrkräfte alle ihre Schülerinnen und Schüler hin. Die Persönlichkeitsrechte der Schülerinnen und Schüler sowie der Lehrkräfte und das Recht am eigenen Bild stehen hier im Vordergrund.

Moodle

Nutzungsbedingungen

Herzlich willkommen auf der Lernplattform des Gymnasium Allermöhe! (Kurz: Moodle GymAll) Bevor Sie Moodle GymAll nutzen, lesen Sie bitte die folgende Datenschutzerklärung. Bei Fragen dazu wenden Sie sich bitte an die Administration unter der E-Mail Adresse thies.henken@gymall.de.

1. Teilnehmer

Wer an Moodlekursen, die zur Begleitung und Ergänzung von Präsenzveranstaltungen eingesetzt werden, teilnehmen möchte, muss sich registrieren. Die Registrierung kann nur über eine Schuladresse des Gymnasium Allermöhe (Vorname.Nachname@gymall.de) oder der Schulbehörde Hamburg (Eduport, BSB) erfolgen. Falls Sie sich mit einer anderen Adresse registrieren möchten, kontaktieren Sie bitte die Administration - das sind derzeit Herr Henken und Herr Lee.

Für den Fall, dass der/die Nutzer/in minderjährig ist, ist eine Registrierung nur mit Zustimmung der Eltern/Erziehungsberechtigten gestattet. Diese muss schriftlich der betreuenden Lehrkraft vorliegen.

Sobald Sie sich registrieren oder die Seite anderweitig nutzen, übermitteln Sie an Moodle Daten, die von der Plattform verarbeitet und möglicherweise auch gespeichert werden. Dies ist zum Beispiel die IP-Adresse, der Nutzername (sofern Sie eingeloggt sind), die Nutzungsdauer und ähnliches. Es handelt sich hierbei teilweise um personenbezogene Daten. Darum gilt auch für uns die Datenschutzgrundverordnung der EU und das Datenschutzgesetz der Bundesregierung Deutschland. Unserer Informationspflicht über Art und Umfang der Erhebung von personenbezogenen Daten und Art und Weise ihrer weiteren Verarbeitung kommen wir mit diesem Schreiben nach, für weitere Details kontaktieren Sie bitte die Administration.

Als registrierter Nutzer können Sie die Daten, die Moodle GymAll über sie speichert, in ihrem persönlichen Nutzerprofil einsehen. Sie können Ihre Profildaten editieren und um freiwillige Angaben ergänzen. Bitte denken Sie stets daran, dass die Profildaten für alle Nutzer der Plattform einsehbar sind. Ihre Emailadresse wird standardmäßig allen Nutzern angezeigt, die im selben Kurs eingeschrieben sind.

Sie sind verpflichtet, Ihre Zugangsdaten geheim zu halten und nicht an Dritte weiterzugeben. Sie haften für jeglichen Missbrauch ihres jeweiligen Accounts, der aufgrund ihres Verschuldens entsteht.

Wenn Moodle GymAll ohne Registrierung genutzt wird, erfolgt ein Login als Gast. Auch hierbei wird die IP-Adresse aus technischen Gründen erhoben. Sie können ausschließlich vom Administrator und nur zu Support-Zwecken eingesehen werden, siehe Punkt 12 der Datenschutzhinweise.

2. Kurse

Kurse werden von Lehrkräften erstellt und können zugangsbeschränkt sein. Die Zugangsschlüssel zu den Kursen geben allein die Lehrkräfte in den zugehörigen Präsenzveranstaltungen aus. Im Missbrauchsfall können die Zugangsschlüssel geändert werden. Die Weitergabe von Zugangsdaten jedweder Art in Social-Media-Plattformen oder via unverschlüsseltem Mailverkehr ist untersagt. Die Rolle eines/einer Lehrkraft können nur Lehrkräfte erhalten, die auf die Datenschutzrichtlinien verpflichtet wurden und der Administration persönlich bekannt sind.

Sie können sich jederzeit aus einem Kursraum als Nutzer/in wieder austragen. Falls die Kursteilnahme von Ihrer Lehrkraft als verpflichtend vorgegeben wurde, wird ein selbstständiges Austragen dieselben Konsequenzen wie ein unentschuldigtes Fehlen nach sich ziehen können.

3. Urheberrechten und anderen gesetzlichen Vorgaben - Pflichten des Nutzers/der Nutzerin

Sie sind zur Einhaltung der Gesetze, insbesondere zur Wahrung von Persönlichkeits-, Urheber-, Leistungs- und Markenschutzrechten verpflichtet. Es ist darüber hinaus nicht gestattet, die Lernplattform für Werbe- und Marketingbotschaften zu verwenden. Sie sind verantwortlich für die Materialien, die Sie in das Moodle hochladen oder anderweitig einbringen (Feeds, Links, Material, Chatbeiträge usw.). Beachten Sie dabei stets das geltende Urheberrecht. Sie sind auch verpflichtet, das Urheberrecht der in Moodle erstellten Inhalte der anderen Nutzerinnen und Nutzer zu wahren. Die Betreiberin wird von Ansprüchen Dritter in diesem Zusammenhang freigestellt, Ansprüche werden an Sie weitergeleitet werden. Ausgenommen ist die unvermeidliche Herstellung automatischer temporärer Kopien durch den verwendeten Browser, das Ausdrucken von Inhalten zu privaten Lernzwecken und Materialien unter freien Lizenzen.

Straftaten, Ordnungswidrigkeiten, insbesondere rassistische, diskriminierende oder gewalttätige Aussagen, und andere, den Lernkontext störende Handlungen sind verboten, insbesondere Beleidigungen, Verleumdungen und Bedrohung. Sie haben sich stets an die Jugendschutzvorschriften zu halten. Beachten Sie insbesondere, dass es sich bei dieser Lernplattform um eine Plattform handelt, auf der auch Minderjährige aktiv sind.

Sie verpflichten sich darüber hinaus, keine Anwendungen auszuführen, die zu einer Veränderung der Datenstruktur von Moodle führen können.

Datenschutzhinweise

1. Freiwilligkeit

Die Benutzung von Moodle ist Ihnen grundsätzlich freigestellt. Verpflichtungen zur Nutzung sind mit der entsprechenden Lehrkraft zu klären.

2. Verarbeitung personenbezogener Daten

Es werden von Moodle GymAll die nachfolgend genannten personenbezogenen Daten verarbeitet: Bei jedem Betreten und Nutzen der Webseite werden die IP-Adresse und die besuchten Seitenelemente verarbeitet und gespeichert. Dies ist nötig, um den Dienst zur Verfügung zu stellen und warten zu können. Alle Log-Daten werden nach einem Halbjahr (30 Wochen) automatisch gelöscht. Die Dauer der Speicherung resultiert aus der im deutschen Schulsystem üblichen Bewertungszyklen, für die eine Prüfung von Aussagen zur Teilnahme an Kurselementen notwendig sein könnte und daher möglich sein muss.

Bei Ihrer Registrierung in Moodle werden Ihr Nachname, Ihr Vorname sowie Ihre E-Mail-Adresse in die Moodle-Datenbank übertragen. Vor- und Nachname dürfen dabei keine Pseudonyme sein, um den reibungslosen Schulablauf auch im digitalen Raum zu gewährleisten. In ihrem jeweiligen persönlichen Profil können Sie Personenbeschreibung, Bild und weitere Daten freiwillig angeben. Ihre Rolle (Lehrer/in oder Schüler/in) sowie die oben genannten Daten können von Lehrkräften und anderen Teilnehmer/innen eingesehen werden. Die Sichtbarkeit der E-Mail-Adresse im Nutzerprofil für andere Nutzerinnen & Nutzer kann eingestellt werden: sie kann ausgeblendet werden, nur für Teilnehmer/innen der von Ihnen belegten Kurse oder für alle Nutzerinnen & Nutzer sichtbar sein. Für Administratoren und Dozierende ist Ihre E-Mail-Adresse im Nutzerprofil immer sichtbar. Ebenso werden Angaben zu Land und möglicher Webseite durch Moodle systemseitig abgefragt. Diese Angaben sind alle freiwillig. Das Gymnasium Allermöhe teilt diese personenbezogenen Daten nicht mit Dritten - davon ausgenommen sind die Daten, die gemäß Vertrag an den Provider Contabo übermittelt werden müssen, um den Dienst bereitstellen zu können. Kurse und Kursinhalte dürfen nicht

veröffentlicht werden, es sei denn, es handelt sich um einen öffentlich zugänglichen Kurs oder es liegt eine ausdrückliche Erlaubnis des Nutzers/der Nutzerin vor, der bzw. die diesen Inhalt verfasst hat. Werden Kurse und Kursinhalte erneut verwendet, müssen beim Export alle Nutzerdaten entfernt werden.

3. Chat

Der Chat ermöglicht eine Kommunikation in Echtzeit. Nachrichten, die Sie im Chat einbringen, sind mit dem Tag und der Uhrzeit des Beitrags, Ihrem Namen und soweit Ihr Profil ein Bild enthält auch mit diesem für alle Kursteilnehmer/innen sichtbar. Chatsitzungen werden als Protokoll gespeichert und können vom Kursbetreuer und der Administration eingesehen werden. Es obliegt der Lehrkraft, hier eine angemessene Lösungsfrist einzustellen.

4. Foren

In Foren können Sie zeitversetzt mit anderen Kursteilnehmern und Teilnehmerinnen kommunizieren. Die Beiträge sind mit Datum und Uhrzeit des Beitrags, Ihrem Namen und soweit Ihr Profil ein Bild enthält auch mit diesem für alle Kursteilnehmerinnen & Kursteilnehmer sichtbar. Beiträge, die Sie z. B. innerhalb von Foren verfassen, sind auch zu einem späteren Zeitpunkt, wenn Sie nicht mehr als Nutzer/in aktiv sind, verfügbar. Diese Beiträge sind vergleichbar mit Leserbriefen in einer Zeitung. Nach der Veröffentlichung kann man diese auch Jahre später noch nachlesen, sofern der Kurs nicht gelöscht wurde.

5. Mitteilungen

Wenn Sie sich als Nutzer/in in Kurse eintragen, erhalten Sie aus diesen Kursräumen Nachrichten per E-Mail. In Ihrem persönlichen Profil können Sie dazu die Einstellungen anpassen. (z. B. Einzel-E-Mails oder tägliche Zusammenfassungen der von Ihnen abonnierten Foren) Lehrkräften steht in ihren Kursen und Arbeitsgruppen eine Liste der Teilnehmer/innen für Sammelmitteilungen zur Verfügung.

6. Glossar und Wiki

Beiträge im Glossar und im Wiki sind mit dem Tag, der Uhrzeit des Beitrags, Ihrem Namen und soweit Ihr Profil ein Bild enthält auch mit diesem versehen und für die anderen Moodle- Nutzerinnen & Nutzer sichtbar. In öffentlichen Kursen schließt dies auch alle Gastzugänge mit ein. Beiträge in Wiki-Aktivitäten in offenen Kursen unterliegen der offenen Lizenz [CC-BY SA 4.0 International](https://creativecommons.org/licenses/by-sa/4.0/) unterliegen und können als solche von anderen Personen in und außerhalb des Moodles geteilt, bearbeitet und verwendet werden. Beachten Sie hierzu die Ansage der betreuenden Lehrkraft im Kurs.

7. Logdaten

Über die in der Anmeldung selbst angeforderten o. g. Informationen hinaus protokolliert die zugrunde liegende Software Moodle, zu welcher Zeit welche Nutzerinnen & Nutzer auf welche Bestandteile der Seite und auf welche Profile anderer Nutzerinnen & Nutzer zugreifen. Protokolliert wird ferner je nach Ausgestaltung des einzelnen Angebots, ob Sie gestellte Aufgaben erledigt, ob und welche Beiträge Sie in den eventuell angebotenen Foren geleistet und ob und wie sie in Workshops oder Tests mitgewirkt haben. Die Logdaten sieht jede/r Teilnehmer/in bezüglich seiner/ihrer eigenen Daten. Lehrkräfte haben Zugriff auf Testergebnisse und andere Rückmeldungen aus den angebotenen Aktivitäten. Logdaten werden gelöscht, wenn der Kurs gelöscht wird. Dies obliegt der Verantwortung der betreuenden Lehrkraft.

8. RSS-Feeds u.a.

Externe Informationen können nicht nur durch Links/Verweise auf Drittsysteme kenntlich und aktiv nutzbar gemacht werden, sondern auch beispielsweise als Bilddatei, IFrame o. Ä. aus anderen Webangeboten (z.B. RSS-Feeds) direkt in eine Moodle-Seite eingebunden sein. In diesem Fall übermittelt Ihr Browser auch an das Drittsystem Daten.

9. Löschung von Daten

Die Registration wird nach Ablauf von 52 Wochen Inaktivität ausgesetzt, der Account wird anschließend mit einer Warndauer von 60 Tagen automatisch gelöscht. Wünschen Sie eine raschere Löschung, können Sie dies jederzeit per Mail bei der Administration beantragen. Sie werden über beide Prozesse per Mail informiert. Profildaten, die Sie zur Gestaltung Ihres Profils freiwillig eingegeben haben, können Sie jederzeit selbst löschen. Die Löschung eines Kurses kann jederzeit durch die Lehrenden veranlasst werden. Damit werden auch die Beiträge der Lernenden innerhalb des Kurses gelöscht. Beiträge und Kommentare in Foren, Wikis und im Glossar sowie von bereit gestellten Dateien sind auch nach der Deaktivierung Ihres Moodle-Zugangs für andere Nutzerinnen & Nutzer abrufbar, bis der entsprechende Kurs oder die entsprechenden Aktivitäten gelöscht wird. Logdaten werden nach einem Halbjahr (30 Wochen) dauerhaft gelöscht. (Zuvor bleiben sie erhalten, um eventuelle Nachfragen zu Bewertungen beantworten zu können.)

10. Datensicherheit

Die Kommunikation mit Moodle GymAll erfolgt über eine verschlüsselte und authentifizierte Verbindung. Die Kursräume sind vor der Indizierung durch Suchmaschinen geschützt. Zur eventuell erforderlichen Wiederherstellung des Systems wird ein Backup mit einer festen Aufbewahrungszeit erstellt. Der Serverstandort ist in der EU, der Serverbetreiber contabo.com. Der Server wird gemietet von dem Gymnasium Allermöhe. [Contabo.com](https://www.contabo.com) speichert Ihre IP 7 Tage, alle anderen Serverlogs 4 Wochen. Grundlage hierfür ist DSGVO §6 Absatz b und c - es ist notwendig, um die Serverdienstleistung anbieten und warten zu können und entspricht den gesetzlichen Aufbewahrungspflichten.

11. Cookies

Moodle GymAll speichert in Ihrem Browser temporär einen Cookie, der Ihren Log-In-Status verwaltet. Dies muss zugelassen werden, da Sie sich sonst für jede Handlung erneut anmelden müssten. Der Cookie wird mit Beendigung der Browsersession gelöscht.

12. Administration

Administratoren haben Zugang zu allen in der Lernplattform entstehenden Daten. Sie dürfen davon nur im eng begrenzten Rahmen ihrer Aufgaben Gebrauch machen. Im Administrationsprozess werden keine personenbezogenen Daten an Dritte weitergeben, auch nicht in anonymisierter Form. Gesetzliche Übermittlungspflichten bleiben davon unberührt.

13. Auskunfts- und Berichtigungsrecht

Nach dem deutschen Datenschutzgesetz haben Sie das Recht, Auskunft über die zu Ihrer Person gespeicherten Daten zu beantragen und/oder unrichtig gespeicherte Daten berichtigen zu lassen. Wenden Sie sich hierzu bitte an die Administration.

14. Haftungsausschluss

Das Gymnasium Allermöhe ist Diensteanbieter der Lernplattform im Sinne des § 10 Telemediengesetz. Das Bereitstellen der Plattform erfolgt nach dem Hamburger Schulgesetz, §98b. Der Betreiber ist danach für die fremden Informationen, die Sie in Moodle übermitteln oder zu denen Sie Zugang zur Nutzung in Moodle gewähren, grundsätzlich nicht verantwortlich. Etwas anderes gilt nur dann, wenn

der Betreiber als Dienstanbieter Kenntnis von den rechtswidrigen Handlungen oder Informationen erhält und nicht unverzüglich tätig wird, um diese Informationen zu entfernen oder den Zugang zu ihnen sperren, sobald Sie Kenntnis erlangt haben. Der Betreiber macht sich darüber hinaus Inhalt, der innerhalb seines Angebots per Hyperlinks durch Nutzende von Moodle zugänglich gemachten fremden Websites ausdrücklich nicht zu eigen und kann deshalb für deren inhaltliche Korrektheit, Vollständigkeit und Verfügbarkeit keine Gewähr leisten. Für rechtswidrige Inhalte der hinter den Hyperlinks befindlichen Internetseiten haftet der Betreiber ebenfalls nicht.

Einwilligungserklärung

Mit der Registrierung und Nutzung von <https://moodle.gymall.de> geben Sie in Kenntnis der obenstehenden Nutzungsbedingungen und Datenschutzhinweise Ihre Einwilligung zu der bezeichneten Datenerhebung und -verwendung. Diese Einwilligung können Sie jederzeit widerrufen. Damit wird Ihr Nutzungszugang gelöscht. Schreiben Sie dazu eine E-Mail an: thies.henken@gymall.de oder wenden Sie sich an Herrn Henken .

Nutzungsregelungen für WLAN-Zugang und Internet-Nutzung an unserer Schule

Das **Gymnasium Allermöhe** eröffnet seinen Schülerinnen und Schülern im Bereich des Schulgeländes als freiwilliges Angebot auf Antrag kostenlos den Zugang zum Intranet und Internet über ein WLAN, wenn die folgenden Regelungen anerkannt werden. Diese sind Teil der Schulordnung. Zudem ist die Nutzung im Schulgesetz (§98) geregelt⁹.

Ein Anspruch auf Zulassung zur Internetnutzung besteht nicht. Das freiwillige Angebot der Internet-Nutzungsmöglichkeit kann individuell oder generell durch die Schule eingeschränkt werden.

Mit der Beantragung eines Zugangs sind folgende Regelungen zu beachten:

Die Regelungen gelten für private und für befristet durch die Schule zur Nutzung überlassene Geräte:

1. Der Zugang zum Internet darf nur für schulische Zwecke genutzt werden. Die Nutzung des Zugangs ist ausschließlich auf Recherche- bzw. Darstellungszwecke für schulische Zwecke begrenzt. Die gesetzlichen Vorschriften zum Jugendschutzrecht, Urheberrecht und Strafrecht sind zu beachten. Insbesondere dürfen keine Urheberrechte an Filmen, Musikstücken o.Ä. verletzt werden, z.B. durch die Nutzung von Internet-Tauschbörsen.
2. Die WLAN-Nutzung beschränkt sich auf maximal 3 technisch identifizierbare Geräte (MAC-Adressen) pro Schülerin oder Schüler.
3. Der Zugang zum WLAN ist nur personenbezogen in Kombination von MAC-Adresse des eingesetzten Gerätes und zugehörigem Passwort bzw. mit Hilfe des eduPort-Benutzerkontos möglich. Es ist untersagt, diese Daten Dritten zugänglich zu machen; im Zweifelsfall haftet der registrierte Nutzer/die registrierte Nutzerin für unzulässige Aktivitäten Dritter bei der Nutzung seines/ihres WLAN-Zugangs.
4. Nutzungseinschränkungen durch das Vorhandensein von Jugendschutzfiltersoftware der Schule sind zu akzeptieren. Der Versuch, die technischen Filtersperren zu umgehen, kann zum Entzug der Nutzungserlaubnis führen.
5. Die Schule übernimmt keine Haftung für die Datensicherheit der von den Schülerinnen und Schülern genutzten privaten Geräte. Die Verantwortung hierfür liegt ausschließlich bei den Nutzerinnen und Nutzern.
6. Manipulationsversuch an der Netzinfrastruktur können zivil- und strafrechtlich verfolgt werden.
7. Die Nutzungsaktivitäten der Schülerinnen und Schüler werden personenbezogen protokolliert und gespeichert¹⁰. Diese können im Fall der missbräuchlichen Nutzung des Zugangs¹¹ von der Schule oder einem von ihr beauftragten Dienstleister ausgewertet oder personenbezogen an Strafverfolgungsbehörden übermittelt werden.

⁹ Hamburger Schulgesetz:

<https://www.hamburg.de/contentblob/1995414/5b23ded37092b4e61d0716878dba9bae/data/schulgesetzdownload.pdf> S. 102ff.

¹⁰ Die entsprechenden Vorgaben der zuständigen Datenschutz-Aufsichtsbehörde sind für die Schule bindend,

¹¹ im Rahmen von Ermittlungsverfahren ist die Schule ggfs. verpflichtet, diese Daten den Ermittlungsbehörden zur Verfügung zu stellen.

8. Wenn im Verdachtsfall die gespeicherten Protokolldaten ausgewertet werden, dann erfolgt die Auswertung durch die von der Schulleitung schriftlich bestimmten Personen. Dabei wird das Vier-Augen-Prinzip eingehalten. Die Auswertung der Protokolldaten wird schriftlich dokumentiert.

Der Widerruf der Einwilligungserklärung kann ohne die Angabe von Gründen jederzeit erfolgen.