Gymnasium
Groß Ilsede

Nutzervereinbarung zur digitalen Datenverarbeitung für den Unterricht
(WLAN, IServ, mobile Endgeräte, MDM)

Stand September 2023

Inhalt

1. Vorwort

Sehr geehrte Erziehungsberechtigte, liebe Schülerinnen und Schüler, auf den folgenden Seiten finden Sie / findet Ihr wichtige Informationen zum Datenschutz wie Nutzungsvereinbarungen, Regelungen, Einwilligungen. Zu verschiedenen schulischen Zwecken muss die Schule

Gymnasium Groß Ilsede, Am Schulzentrum 35, 32421 Ilsede

Schulleitung: Malte Holthusen

Datenschutzbeauftragte: Stefan Kretschmer und Thomas Müller

E-Mail: datenschutz@ggilse.de

personenbezogene Daten verarbeiten. Dafür ist eine Einwilligung der Betroffenen notwendig. Sie können die Informationen auf der Homepage jederzeit einsehen bzw. das Dokument in unserem Sekretariat auf Wunsch als Ausdruck erhalten. Die letzte Seite muss von den Schülerinnen und Schülern und Erziehungsberechtigten unterzeichnet werden und ist Bestandteil der Schülerakte.

2. Nutzung des schuleigenen WLAN

Alle Nutzer sind berechtigt, das schuleigene WLAN zu nutzen. Die SSID lautet

GGI-ISERV

Der Benutzeraccount und das Passwort entsprechen dem IServ-Account. Das WLAN ist ausschließlich für den schulischen Gebrauch vorgesehen. Die Schule behält sich vor, private Geräte, die nicht zu schulischen Zwecken genutzt werden (Handys, Smartwatches,…), vom WLAN auszuschließen. Folgende Daten werden während der Nutzung von unserem WLAN-System verarbeitet:

- Nutzer
- Login und -out
- Gerätetyp
- MAC-Adresse
- IP-Adresse
- Standort

Die Logindaten (Datum, Uhrzeit, Nutzer, MAC-Adresse, IP-Adresse) werden im Logfile für 7 Tage protokolliert.

3. Informationen über die Nutzung der Lernplattform IServ

Das Gymnasium Groß Ilsede stellt seinen Schülerinnen und Schülern (im Folgenden: Nutzer genannt) als Kommunikations- und Austauschplattform IServ zur Verfügung.

Die Schule ist dabei strengen datenschutzrechtlichen Vorgaben unterworfen, für deren Einhaltung sie verantwortlich ist.

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.

IServ ist am Gymnasium Groß Ilsede als **digitales Lehrmittel zur Kommunikation** eingeführt. Jeder Nutzer ist verpflichtet, täglich (an Schultagen) seine Mails und Aufgaben hierüber abzurufen und sich ab 15:30 Uhr über den Vertretungs- und der Veranstaltungsplan über Änderungen am Unterrichtsablauf zu informieren. Alle Klausuren sind im Klausurplan und alle wichtigen, schulischen Termine im Kalender eingetragen.

Die IServ-Oberfläche ist über das Web unter der Adresse https://www.ggilse.de/ oder über unsere Homepage zu erreichen. Zum Abrufen über ein Mobilgerät empfehlen wir die kostenfreie IServ-App.

Alternativ können zu den Öffnungszeiten die PCs in unserer Studienbücherei genutzt werden.

3.1 Nutzungsmöglichkeiten – IServ

Der Schulserver ist nur für registrierte Benutzer mit persönlichem Passwort erreichbar. Im Wesentlichen sind dies die Schülerinnen und Schüler, deren Eltern, die Lehrkräfte und die Verwaltungsmitarbeiterinnen des Gymnasiums. In Einzelfällen kann auch externen Personen (Schulbegleitung, Projektmitarbeiter) ein Zugang eingeräumt werden.

Die Schule entscheidet darüber, welche Module von IServ für den innerschulischen Gebrauch für welche Gruppen freigeschaltet werden.

Neben dem E-Mail-Verkehr zwischen Schülern, Lehrern und der Schulverwaltung können Klassenarbeits- und Klausurtermine, Vertretungs- und Veranstaltungspläne, Speisepläne der Mensa, Hofdienste und Termine der Zeugniskonferenzen eingesehen werden. Über die Module Druckmanagement, Projektwahl und Aufgaben können die Drucker in der Schule verwendet, die Wahlen zur Projektwoche durchgeführt oder aus dem unterrichtlichen Zusammenhang Aufgaben organisiert werden. Ferner bietet IServ die Module Videokonferenzen und Schulbuchausleihe. Viele weitere Module sind verfügbar.

3.2 Kommunikation über IServ

E-Mail

Die Schule stellt den Nutzern einen persönlichen E-Mail-Account zur Verfügung. Dieser darf nur für die schulische Kommunikation (interner Gebrauch) verwendet werden. Die Schule ist damit 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 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.

Massen-E-Mails, Joke-E-Mails oder ähnliches sind nicht gestattet.

Die schulische E-Mail-Adresse darf nicht für private Zwecke zur Anmeldung bei Internetangeboten jeder Art verwendet werden. Das gilt insbesondere für alle sozialen Netzwerke wie z. B. Facebook oder Google+.

Eine Weiterleitung an private E-Mail-Adressen ist nicht erlaubt.

Chat/Messenger

Die Schule stellt eine Chat-Funktion zur Verfügung stellt. Es gelten dieselben Vorgaben wie bei der E-Mail-Nutzung.

Forum

Die Schule stellt eine Forum-Funktion zur Verfügung. Es gelten dieselben Vorgaben wie bei der E-Mail-Nutzung.

Darüber hinaus sind die Moderatoren und Administratoren der Foren berechtigt, unangemessene Beiträge zu löschen.

Die Nutzer verpflichten sich, in Foren, Messenger, Chats und von IServ aus versendeten E-Mails die Rechte anderer zu achten.

Die Foreninhalte können am Schuljahresende gelöscht werden.

Kalender

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

Aufgaben

Aufgaben können über IServ gestellt werden. Die Lehrkräfte achten dabei auf einen angemessenen Bearbeitungszeitraum.

Videokonferenz

Videokonferenzen können im Rahmen des Unterrichts oder von Veranstaltungen und Projekten am GGI durchgeführt werden. Sie können anstelle des Unterrichts oder zur Ergänzung veranstaltet werden.

Damit Videokonferenzen sinnvoll durchgeführt werden können und sich alle Beteiligten wohlfühlen, wünschen wir uns die Beachtung der folgenden 10 Punkte:

1. Alle eingeladenen Schülerinnen und Schüler nehmen an der Videokonferenz so teil, wie sie auch am Unterricht bzw. am Projekt teilnehmen würden. Für den Unterricht per Videokonferenz bedeutet das: Alle sind ordentlich angezogen, sitzen an einem Tisch und haben die Arbeitsmaterialien in Reichweite. Essen gehört nicht auf den Arbeitsplatz.
2. Das genutzte digitale Gerät ist so einsatzbereit, dass Mikrofon und Kamera funktionieren. Die Lehrkraft entscheidet je nach Situation über die Nutzung und gibt entsprechende Anweisungen. Sollte es technische Probleme geben, wird die Lehrkraft darüber in der Konferenz per Chat notfalls umgehend per Mail informiert.
3. Unterricht über Videokonferenz bedeutet, dass man sich nur darauf konzentriert! Es werden keine Nebentätigkeiten ausgeführt.
4. Die üblichen Gesprächs- und Höflichkeitsregeln gelten auch im Videounterricht. Dies gilt auch für die Pünktlichkeit.
5. Videokonferenzen werden nicht absichtlich gestört oder verzögert.

6. Die Chatfunktion sollte nur entsprechend der Anweisungen durch die Lehrkraft oder bei technischen Problemen benutzt werden.
7. Das Speichern oder Aufnehmen der Videokonferenzen (z. B. Screenshots, Fotos, Videos) ist grundsätzlich verboten. Es verstößt gegen das KUG (Kunst- und Urhebergesetz §§ 22 und 33) und das StGB (§ 201 Verletzung der Vertraulichkeit des Wortes).
8. Die absichtliche Teilnahme Dritter an den Videokonferenzen ist nicht gestattet! Dies gilt besonders für das absichtliche Mithören oder Dokumentieren von Videokonferenzen. Hierbei handelt es sich um eine Verletzung der Vertraulichkeit des Wortes gemäß § 201 Abs. 1 und Abs. 2 StGB. Darüber hinaus wird hierdurch das Lehrer-Schüler-Vertrauensverhältnis empfindlich gestört. Selbstverständlich gilt dies nur für absichtliches Handeln und nicht für kurzzeitige Anwesenheit im Rahmen des gemeinsamen Lebensortes. Im Falle von Unterstützungsleistungen während der Videokonferenz, teilt der Betroffene der Lehrkraft die Anwesenheit der Unterstützungskraft mit.
9. Es ist grundsätzlich verboten, jegliche Inhalte, die jugendgefährdend sind und/oder nicht mit den freiheitlich demokratischen Grundwerten der BRD übereinstimmen, im Rahmen der Videokonferenz aufzurufen, zu versenden oder zu verbreiten.
10. Sollte eine Videokonferenz versäumt werden, gelten die gleichen Regeln wie im Präsensunterricht: Das Sekretariat oder der entsprechende Lehrer sind umgehend per Mail zu informiert, eine elterliche Entschuldigung erfolgt beim Klassenlehrer, bzw. beim Tutor.

3.3 Moderatoren und Administratoren IServ

Für die Gruppenforen können Moderatoren eingesetzt werden, die Forumsbeiträge auch löschen können. Moderatoren dürfen nur in dem ihnen anvertrauten Forum moderieren.

Die Schulleitung bestimmt Administratoren. Dabei handelt es sich um Lehrkräfte des Gymnasiums. Die Administratoren haben weitergehende Rechte, verwenden diese aber grundsätzlich nicht dazu, sich Zugang zu persönlichen Konten bzw. persönlichen Daten zu verschaffen.

Sollte ein Nutzer sein Passwort vergessen haben, ist er verpflichtet, das durch einen Administrator neu vergebene Passwort beim nächsten Einloggen sofort zu ändern.

Nur der Nutzer selbst darf ein neues Passwort für sich persönlich bei einem Administrator beantragen. Nur in Ausnahmefällen können neue Passwörter über die Erziehungsberechtigten beauftragt werden.

Chat-Protokolle sind auch für Administratoren grundsätzlich nur lesbar, wenn ein Verstoß per Klick auf die entsprechende Schaltfläche gemeldet wurde.

Der Schulträger bestimmt weitere Administratoren, die ausschließlich technischen Support leisten. Sollten diese externen Administratoren oder Supportmitarbeiter der IServ GmbH an Problemen arbeiten, die die Nutzeraccounts betreffen, werden die betroffenen Nutzer hierüber im Vorfeld informiert.

Bei technischen Problemen sind die Administratoren berechtigt, die Logfiles auszuwerten.

3.4 Datennutzung von IServ

Zu jedem Nutzer speichert IServ folgende Daten, die zur Nutzung des Accounts notwendig sind:
(erster) Vorname und Nachname

Hieraus generiert IServ den Account und die E-Mail Adresse:

vorname.nachname
vorname.nachname@ggilse.de

Außerdem wird das Benutzerpasswort als Prüfziffer gespeichert.

Für die Schulorganisation sinnvolle und notwendige Daten:

Zugehörigkeit zu Jahrgang, Klasse und Kursen
Schülernummer

Zur Dokumentation des Systems notwendige Daten:

Log-Daten aller Anmeldeversuche mit IP-Adresse und Zeitstempel

Log-Daten der Systemauslastung

Alle Daten, die der Nutzer dem System übergibt:

- Daten, die der Nutzer in seinem Account (Home- bzw. Files-Verzeichnis) speichert
- Daten, die der Nutzer im Gruppenordner speichert
- Daten, die der Nutzer im Aufgabenordner hochlädt
- Mails, die der Nutzer versendet.
- Beiträge, die der Nutzer im Forum-, Chat- oder Messengermodul postet
- Eingaben, die der Nutzer in gemeinsam genutzten Texten macht
- Störungsmeldungen, die der Nutzer abgibt
- Kalendereinträge, die der Nutzer vornimmt
- Antworten, die der Nutzer in Umfragen gibt
- Antworten, die der Nutzer bei der Kurswahl macht
- Daten, die der Nutzer in seinem Adressbuch einträgt
- Daten, die der Nutzer in seinem Profil einträgt
- Druckaufträge, die der Nutzer über IServ abgibt

Weitere Nutzerbezogene Daten werden nicht im IServ-System gespeichert. Besonders schützenswerte Daten (Geschlecht, Religionszugehörigkeit, Abstammung,…) werden nicht von IServ erfasst.

Für die Schulbuchausleihe werden folgende Daten (ggf. zusätzlich) erfasst:

1. Geburtsdatum des Schülers (zur Überprüfung der Volljährigkeit)
2. Ggf. Name und Anschrift eines Erziehungsberechtigten
3. Ggf. gestellte Anträge zur Vergünstigung
4. Laufende Daten über vorbestellte und ausgeliehene Bücher
5. Ggf. offene Forderungen aus der Schulbuchausleihe

Weitere Informationen über die Datenverarbeitung und die Datenschutzbestimmungen des IServ-Systems sind auf der Webseite des Herstellers abrufbar: https://www.iserv.de

3.5 Abrufbarkeit der Daten und Löschung des Accounts und Daten

1. Zu jedem Account gehören ein eigener Datenbereich (Home- bzw. Files-Verzeichnis) und ein Mailbereich. Daten in diesem Bereich sind nur vom Nutzer selbst abrufbar.
2. Jeder Nutzer ist Mitglied in verschiedenen Gruppen (Jahrgangsgruppen, Klassengruppen, Kursgruppen, etc.). Auch diese Gruppen haben Datenbereiche und Foren. Diese sind für alle Gruppenmitglieder freigegeben.
3. Ferner gibt es öffentliche Bereiche (öffentliche Foren). Hierauf haben alle aktiven Nutzer Zugriff.
4. In einzelnen Modulen (Messenger, Aufgabenmodul, Texte…) lassen sich die Zugriffsrechte individuell steuern.

Beim Verlassen der Schule wir der Account gelöscht. Die Schule informiert den Nutzer hierüber mindestens 14 Tage im Voraus. Beim Löschen des Accounts werden sämtliche vom Nutzer abgelegten Daten, Adressbucheinträge, Druckaufträge und Mails gelöscht. Der Nutzer ist für die rechtzeitige Sicherung seiner Daten selbst verantwortlich. Daten in unterschiedlichen Modulen (Foren, Aufgabenmodul,…) bleiben evtl. bis zum Schuljahresende anonymisiert gespeichert.

1. Gruppenordner werden zu Beginn eines jeden Schuljahres auf ihre Notwendigkeit überprüft. Nicht mehr benötigte Ordner, werden im Rahmen dieser Überprüfung gelöscht.
2. Gelöschte Benutzer sowie deren gespeicherte E-Mails, Adressbucheinträge, Druckaufträge oder persönliche Dateien werden spätestens nach 90 Tagen endgültig gelöscht.
3. Gelöschte E-Mails werden nach ca. 7 Tagen endgültig aus dem Ordner „Gelöscht“ entfernt.
4. Die Chatprotokolle werden für 3 Monate aufbewahrt.
5. Die Anmeldeversuche am Server werden für 6 Monate, Webproxy-Log-Dateien und Firewall-Log-Dateien für einige Wochen gespeichert.
6. Forenbeiträge werden dauerhaft gespeichert. Sie können vom Verfasser und den Moderatoren gelöscht werden. Ein entsprechender Hinweis ersetzt dann den Beitrag. Ältere Forenbeiträge werden ausgeblendet und sind nur noch über die Archiv-Ansicht aufrufbar.
7. Dateien in Gruppenordnern sowie gruppenbezogene Foren werden 90 Tage nach Löschen der jeweiligen Gruppe endgültig gelöscht.
8. Bearbeitete Aufgaben können von Benutzern (Lehrer) individuell gelöscht werden.
9. Adressbucheinträge können jederzeit verändert werden.

Unabhängig von den angegebenen Löschfristen können Daten noch für längere Zeit auf dem Backupserver vorgehalten werden.

3.6 Verhaltensregeln im Umgang mit IServ und Ahndung bei Verstößen

1. Jeder Nutzer erhält ein **Nutzerkonto (Account)**. 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.
2. Erfährt ein Nutzer, dass ein Dritter Kenntnis von seinem Passwort hat, so ist er verpflichtet, sein Passwort umgehend zu ändern.
3. Die im gemeinsamen **Adressbuch** eingegebenen Daten sind für alle Nutzer sichtbar. Es wird deshalb geraten, so wenig personenbezogene Daten wie möglich von sich preiszugeben.
4. Alle Nutzer sind verpflichtet, eingesetzte **Filter** und Sperren zu respektieren und diese nicht zu umgehen.

5. Die Nutzer verpflichten sich, die **gesetzlichen Regelungen** des Straf- und Jugendschutzgesetzes sowie das Urhebergesetz zu beachten.
   Jegliche Inhalte, die jugendgefährdend sind und/oder nicht mit den freiheitlich demokratischen Grundwerten der BRD übereinstimmen, dürfen nicht über diese Plattform gespeichert oder kommuniziert werden.
   Wer Dateien auf IServ hochlädt, über IServ versendet oder nutzt, tut dies in eigener Verantwortung.
6. Die Schule übernimmt keine Verantwortung für die Inhalte und die Art **gespeicherter Daten**.
7. Die **Sicherung** in IServ gespeicherter Daten gegen Verlust obliegt der Verantwortung der Nutzer.
8. Das **Aufrufen und Speichern** jugendgefährdender und anderer strafrechtlich relevanter Inhalte auf dem Schulserver ist ebenso verboten wie die Speicherung von URLs (Webseiten) oder Links auf jugendgefährdende Websites oder Websites mit strafrechtlich relevanten Inhalten.
9. Weil umfangreiche **Up- und Downloads** (>20 MB) die Arbeitsgeschwindigkeit des Servers beeinträchtigen, sind diese nicht erlaubt. Ausnahmen sind vorab mit den Administratoren abzusprechen.
10. Da der **Speicherplatz** auf unseren Servern begrenzt ist, ist jeder Nutzer aufgerufen, seinen Speicherbedarf auf das nötige zu beschränken. Derzeit sollten Schüleraccounts bis zur 6. Klasse maximal 2 GB belegen. Schüleraccounts aus Jahrgängen mit digitalen Endgeräten in der Sek I sollten maximal 4 GB belegen, Schüleraccounts aus der Sek II sollten maximal 6 GB belegen. Belegt ein Nutzer mehr Speicherplatz, so kann er von den Administratoren zur Freigeben des Speichers aufgefordert werden. Sollte ein Nutzer **zu schulischen Zwecken** mehr Speicherbedarf haben, so ist das den Administratoren anzuzeigen.
11. Nutzer sind verpflichtet, regelmäßig den **Speicherbedarf** ihres Accounts zu **prüfen** und überflüssige oder nicht mehr benötigte Daten und Mails zu löschen.
12. Die Installation oder Nutzung **fremder Software** durch die Nutzer an den schuleigenen Rechnern ist nicht zulässig, sie darf nur von den Administratoren durchgeführt werden.
13. Das IServ-System erstellt **Log-Dateien** (Protokolle), die in begründeten Fällen (Rechtsverstöße, Support,…) von den von der Schulleitung bestimmten Personen und Administratoren ausgewertet werden können.

Im Fall des Verdachts der unzulässigen Nutzung (Regelverletzung, Betrugs- oder Täuschungsversuch - insbesondere im Fall des Verdachts auf Straftaten oder Ordnungswidrigkeiten) kann die Schulleitung im erforderlichen Umfang folgende Maßnahmen durchführen:

- Auswertung der System-Protokolldaten,
- Auswertung der im Zusammenhang mit der Internetnutzung entstandenen Protokolldaten,
- Inaugenscheinnahme von Inhalten der E-Mail-und Chat-Kommunikation.

Welche Protokoll- oder Nutzungsdaten zur Aufklärung des Vorgangs ausgewertet werden, entscheidet im jeweiligen Einzelfall die Schulleitung.

4. Mobile Endgeräte und Verhaltensregeln

Das Gymnasium Groß Ilsede hat sich 2018 entschieden, ab dem 7. Jahrgang digitale Endgeräte (iPads) im Unterricht einzusetzen. Ein entsprechendes Medienbildungskonzept wurde erarbeitet und iPads als digitales Lehrmittel verbindlich (mit Beschluss der Gesamtkonferenz) eingeführt.

Hiermit verfolgen wir die Ziele:

- die Schülerinnen und Schüler im Umgang mit neuen Medien zu schulen und ihre Medienkompetenz zu stärken,
- den Unterricht zu bereichern und anschaulicher zu gestalten,
- die Zusammenarbeit und Kommunikation zu fördern und
- Schülerinnen und Schülern mehr Freiräume zum selbstgestalteten Lernen einzuräumen.

Um diese Ziele zu erreichen, müssen die Schülerinnen und Schüler private iPads nach dem „bring your own device“-Prinzip anschaffen. Diese müssen von der Schule in ein zentrales „Mobile Device Management“, kurz MDM-System, eingebunden werden. Ferner müssen Verhaltensregeln für den Umgang mit den Geräten aufgestellt werden. Dies soll in Form dieser Nutzervereinbarung geschehen.

1. Jeder Nutzer ist verpflichtet, sein Gerät mittels **Zugangscode** von unerlaubtem Fremdzugriff zu schützen.
2. Die Nutzer aktualisieren das **Betriebssystem** (iOS) ihres Gerätes selbstständig.
3. Die Nutzer sorgen dafür, dass die Geräte jeden Tag ausreichend **aufgeladen** und mit genügend Speicherplatz für schulisches Arbeiten mitgebracht werden.
4. Einfache Kopfhörer eine **Tastatur und ein Eingabestift** sind immer mitzubringen.
5. Private Geräte und Wertgegenstände sind in der Schule nicht gegen Verlust, Diebstahl oder Beschädigung versichert. Die privaten iPads können beim Erwerb über die empfohlene Bezugsquelle versichert werden.
6. Alle Nutzer sind verpflichtet, eingesetzte **Filter** und **Sperren** zu respektieren und diese nicht zu umgehen. Geräte, die *„gerootet“* wurden oder auf andere Weise die eingerichteten Schutz- und Wartungsfunktionen umgehen, dürfen im Schulnetzwerk nicht zum Einsatz kommen. Die Schule ist berechtigt, diese Geräte von der Arbeit im Unterricht und dem Zugang zum Netzwerk auszuschließen.
7. Während der Schulzeit muss das Gerät im schuleigenen WLAN angemeldet sein.
8. Die Nutzung von Messengern (z.B. WhatsApp, Facebook etc.) ist während der regulären Schulzeiten aus datenschutzrechtlichen Gründen untersagt.
9. Grundlage der Arbeit mit den Geräten ist die Hausordnung und die Nutzungsordnung der PC-Räume sowie der Studienbücherei. Diese Dokumente sind auf der Homepage zu finden.
10. **In der Schule dürfen nur zu unterrichtlichen und von der Lehrerin / dem Lehrer genehmigten Zwecken Bild-, Video- und Tonaufnahmen angefertigt werden. Ohne das ausdrückliche, schriftliche Einverständnis der Betroffenen, der Erziehungsberechtigten und der Schule dürfen diese nicht veröffentlicht und dauerhaft gespeichert werden.**
11. Die Nutzer haben bei der Benutzung des iPads die Hinweise der Lehrerin / des Lehrers zu beachten. Insbesondere sind der Aufruf und die Speicherung von Dokumenten mit rechtswidrigem oder ehrverletzendem Inhalt sowie deren Verbreitung untersagt. Darüber hinaus dürfen nur die für den Unterricht benötigten und von der Lehrerin / dem Lehrer benannten APPs gestartet werden.

12. Im unterrichtlichen Kontext haben die Lehrerin / der Lehrer jederzeit die Möglichkeit, den Bildschirminhalt des iPad einzusehen oder diesen im Klassenraum zu projizieren sowie gezielt einzelne APPs ferngesteuert zu starten oder das Gerät zu sperren.
13. Rechtsgeschäfte dürfen nicht über das schulische Netzwerk vorgenommen werden. Bei Missbrauch übernimmt die Schule keine Haftung.
14. Bei missbräuchlicher Nutzung durch den Nutzer, betrifft insbesondere Verstöße gegen § 2 NSchG (z. B.: die Verbreitung extremistischer Inhalte), übernimmt die Schule keine Haftung.
15. Die Nutzer verpflichten sich, die **gesetzlichen Regelungen** des Straf- und Jugendschutzgesetzes sowie das Urhebergesetz zu beachten.
    Jegliche Inhalte, die jugendgefährdend sind und/oder nicht mit den freiheitlich demokratischen Grundwerten der BRD übereinstimmen, dürfen nicht gespeichert oder kommuniziert werden.
16. Das **Aufrufen und Speichern** jugendgefährdender und anderer strafrechtlich relevanter Inhalte ist ebenso verboten wie die Speicherung von URLs (Webseiten) oder Links auf jugendgefährdende Websites oder Websites mit strafrechtlich relevanten Inhalten.

5. MDM-System für die Nutzung digitaler Endgeräte

Voraussetzung für eine zentrale Installation von schulischen APPs, Zugangsprofilen zum WLAN und die Nutzung unserer pädagogischen Software zum Klassenraummanagement ist die Einbindung des privateigenen Gerätes in ein zentrales Managementsystem (MDM-Server). Der Schulträger stellt hierzu ein System zur Verfügung, dass auf der Verwaltung von jamf beruht. Die in Deutschland strengen Datenschutzvorschriften werden damit eingehalten. In begrenztem Umfang erhält die Schule damit Zugriff auf personenbezogene Daten. Dies sind insbesondere der Name des iPads, dessen aktuelle IP- und MAC-Adresse sowie die Liste der installierten APPs sowie technische Daten des Gerätes.

Über das System ist eine Ortung des Gerätes technisch möglich, sobald es in den *„lost mode“* versetzt wurde, also als verloren oder gestohlen gemeldet worden ist. Innerhalb der Schule ist eine Ortung über das WLAN möglich.

Die Schule wird den Vornamen, die ersten beiden Buchstaben des Nachnamens, einen Teil der Schülernummer, die Klasse und die Kurszugehörigkeit des Nutzers in das MDM-System einpflegen, damit eine leichte Zuordnung zu den Geräten und der Einsatz im Unterricht möglich wird.

Für die Schule haben ausgewählte Lehrerinnen und Lehrer (MDM-Admins) und Administratoren des Schulträgers Zugriff auf das MDM-System.

Das zentrale MDM erlaubt es der Schule, APPs ferngesteuert zu installieren und von der Schule installierte APPs zu löschen. Mit dem Löschen der APPs werden ggf. auch damit erzeugte Dateien gelöscht, sofern diese nicht extern gesichert wurden.

Von der Schule verwaltete Apps sind mit einer Apple-ID der Schule bzw. des Schulträgers verknüpft.

Der Geräteeigentümer ist berechtigt, mit einer eigenen Apple-ID Apps zu installieren. Auf diese Apps hat die Schule keinen Zugriff. Im Supportfall ist es nötig, dass der Nutzer seine eigene Apple-ID abmeldet.

Derzeit meldet die Schule die Nutzer pseudonymisiert bei Schulbuchverlagen und Softwarefirmen (Anton und Microsoft) an und registriert sie. Ferner meldet sie Schule die Schülerinnen und Schüler bei inländischen Schulbuchverlagen an, wenn zuvor mit diesen ein entsprechender

Datennutzungsvertrag geschlossen wurde (derzeit Bibox von Westermann). Bei anderen Verlagen müssen sich die Nutzer selbst anmelden. Hierüber erfolgt eine gesonderte Information.

Kosten

Für die Bereitstellung des MDM-Servers, den Support und die Anschaffung von APPs fällt eine Gebühr von aktuell maximal 2,- € pro Monat an, die je nach Bedarf von der Schule zentral eingesammelt wird.

Einbindung in das MDM-System

Die problemlose und effiziente Einbindung des privateigenen Gerätes funktioniert nur, wenn dieses zum sogenannten „DEP-Programm“ gehört. Die Zugehörigkeit zum DEP-Programm ist sichergestellt, wenn das iPad über die von der Schule und der Arbeitsgruppe „Endgeräte“ empfohlene Bezugsquelle beschafft wird.

Die Einbindung externer Geräte aus anderen Bezugsquellen ist möglich. Die Einbindung kann aber nicht garantiert werden. Hierzu müssen die Geräte komplett gelöscht und manuell eingebunden werden. Dieser Vorgang ist sehr zeitaufwändig. Der Zugang zu den von der Schule verwalteten Apps kann sich verzögern und der Support der Schule ist (insbesondere bei Hardwareproblemen) stark eingeschränkt.

Mit dem Beenden der Schulzeit am GGI wird das iPad aus dem MDM der Schule entfernt. Dabei muss das Gerät zurückgesetzt werden, wobei sämtliche APPs, Einstellungen und Daten gelöscht werden.
Für eine Datensicherung im Vorfeld ist der Nutzer zuständig.

MDM-Profil

Die Schule installiert über das MDM-System verschiedene Profile, die die Benutzung des Gerätes und seiner Möglichkeiten einschränken. Dabei gibt es ein allgemeines Profil, das immer aktiv ist, und eines für die Benutzung während der Schulzeit. Nähere Angaben stehe im Punkt „Steuerung während der Unterrichtszeit“.

Alle Nutzer sind verpflichtet, eingesetzte Filter und Sperren zu respektieren und diese nicht zu umgehen. Ein eigenständiges Verlassen der entfernten Verwaltung ist nicht zulässig.

Die Schule legt aus organisatorischen Gründen den Gerätenamen des iPads (Vorname und die ersten zwei Buchstaben des Nachnamens) und die Nachricht auf dem Sperrbildschirm (Benutzername, Gerätenummer) fest.

Wesentliche Einschränkungen des allgemeinen Profils: Aus Datenschutzgründen schränke wir das serverseitige Protokollieren ein.

Softwaresteuerung während der Schulzeit

Während der Schulzeit (an Schultagen in der Zeit von 7:45 bis 15:30 Uhr) wird innerhalb des Schulgeländes das Schulprofil aktiviert. Spätestens um 15:30 Uhr wird es deaktiviert.

Wesentliche Einschränkungen des Schul-Profils: Aus Datenschutzgründen dürfen wir an der Schule einige Apple-Dienste wie Siri und iCloud nicht zulassen. Weitere Einschränkungen sind das Verbot mobiler Hotspots und die zwingende WLAN-Anmeldung zu Schulzeiten, um die Geräte während des Unterrichtes zu nutzen. Das Profile enthält auch Einschränkungen, die Jugendliche schützen (FSK-12) sollen. Einen kompletten Schutz kann es aber nicht geben. Privat (auf eigene Apple-ID) installierte Apps und nicht benötigte Systemprogramme werden ausgeblendet. Feathers, die den Schulablauf stören könnten oder den Datenschutz gefährden, können ebenfalls deaktiviert werden.

Während des Unterrichtes können Lehrerinnen und Lehrer die Geräte über die Classroom-App und die jamf-Lehrer-App steuern, überwachen und in den Prüfungsmodus setzen.

Möglichkeiten der Classroom-App: Mit dieser App erhalten Lehrerinnen und Lehrer innerhalb eines Unterrichtsraumes einen Überblick der eingeschalteten Schülergeräte und der darauf gerade aktiven Apps. Lehrerinnen und Lehrer können die Geräte öffnen, auf ihnen navigieren, um Schülern zu helfen, sich den Bildschirm anzeigen lassen, den Bildschirm ausblenden, die Geräte sperren oder stummschalten, den Benutzer abmelden, Airplay steuern und ein Passwort zu setzen. Die aktive Überwachung bzw. Steuerung über Classroom wird den Schülern über ein Symbol angezeigt.

Möglichkeiten der jamf-Lehrer-App: Mit dieser App können Lehrer einstellen, welche Apps und Systemfunktionen auf dem iPad zur Verfügung stehen und welche Webzugriffe sowie Inhalte gezielt gesteuert werden. Die Einschränkungen sind auf die Unterrichtseinheit maximal jedoch auf zwei Stunden beschränkt.

Support

Die Schule administriert die Geräte über das MDM, passt Profile an und aktualisiert die von ihr verwalteten Apps. Diese geschieht normalerweise zu den zuvor angekündigten Zeiten.

Die Nutzer stellen nach Möglichkeit sicher, dass das Gerät zu diesen Zeiten mit Strom versorgt und in ein über das Internet zugänglichen WLAN eingebunden ist. In dringenden Fällen ist die Schule berechtigt, jederzeit auf die Geräte zuzugreifen.

Die Schule bietet im Rahmen ihrer Möglichkeiten Hilfestellung bei Problemen und Fragen zum Gerät an. Diese Hilfestellung ist eine freiwillige Leistung. Es besteht von Seiten der Nutzer kein Anspruch auf eine schnelle, professionelle Hilfe.

In einigen Fällen kann es notwendig sein, dass die eigene Apple-ID abgemeldet wird. Der Nutzer stellt sicher, dass diese Möglichkeit gegeben ist.

Die Schule übernimmt keine Haftung für Datenverlust, der durch den Support der Schule verursacht wurde.

6. Nutzungsvereinbarung für Schülerinnen und Schüler über die Nutzung von Office 365 und die damit verbundene Verarbeitung personenbezogener Daten

Für alle Arbeiten im Unterricht und in Phasen des eigenverantwortlichen Lernens erhalten die Schüler einen Zugang zu Office 365 A1 Education (im Folgenden „Office 365“). Den Zugang zu Office 365 steht auch außerhalb des Unterrichts zur schulischen Nutzung zur Verfügung. Die Nutzung setzt einen verantwortungsvollen Umgang mit den Netzwerkressourcen, der Arbeitsplattform Office 365 sowie den eigenen personenbezogenen Daten und denen von anderen in der Schule lernenden und arbeitenden Personen voraus. Die folgende Nutzungsvereinbarung informiert und bildet die Rahmenbedingungen für eine verantwortungsvolle Nutzung. Die Einwilligung ist Voraussetzung für die Erteilung eines Nutzerzugangs.

Zum Umfang des von der Schule für die Benutzer kostenlos bereitgestellten Paketes gehört der Zugang zu Office 365 A1 Education mit

- Word
- Excel
- Powerpoint
- Teams
- OneNote

Passwörter

- müssen sicher sein und dürfen nicht zu erraten sein. Sie müssen aus mindestens 6 Zeichen bestehen, worunter sich eine Zahl, ein Großbuchstabe und ein Sonderzeichen befinden müssen.
- sollten zumindest einmal im Schuljahr gewechselt werden.

Zugangsdaten

- Der Benutzer ist verpflichtet, die eigenen Zugangsdaten zum persönlichen Office 365 Konto geheim zu halten. Sie dürfen nicht an andere Personen weitergegeben werden.
- Sollten die eigenen Zugangsdaten durch ein Versehen anderen Personen bekannt geworden sein, ist der Benutzer verpflichtet, sofort Maßnahmen zum Schutz der eigenen Zugänge zu ergreifen. Falls noch möglich, sind Zugangspasswörter zu ändern. Ist dieses nicht möglich, ist ein schulischer Administrator zu informieren.
- Sollte der Benutzer in Kenntnis fremder Zugangsdaten gelangen, so ist es untersagt, sich damit Zugang zum fremden Benutzerkonto zu verschaffen. Der Benutzer ist jedoch verpflichtet, den Eigentümer der Zugangsdaten oder einen schulischen Administrator zu informieren.

Datenschutz und Datensicherheit

Der Schulträger stellt unserer Schule die Version Microsoft Office 365 A1 zur Verfügung. Mit Microsoft wurde hierzu ein Vertrag abgeschlossen, welcher gewährleistet, dass personenbezogene Daten von Benutzern nur entsprechend der Vertragsbestimmungen verarbeitet werden. Microsoft verpflichtet sich, die personenbezogenen Daten von Benutzern in Office 365 nicht zur Erstellung von Profilen zur Anzeige von Werbung oder Direkt Marketing zu nutzen. Ziel unserer Schule ist es, durch eine Minimierung von personenbezogenen Daten bei der Nutzung von Office 365 auf das erforderliche Maß, das Recht auf informationelle Selbstbestimmung unserer Schüler und Lehrkräfte bestmöglich zu schützen. Dieses ist nur möglich, wenn die Benutzer selbst durch verantwortungsvolles Handeln zum Schutz und zur Sicherheit ihrer personenbezogenen Daten beitragen und auch das Recht anderer Personen an der Schule auf informationelle Selbstbestimmung respektieren.

Zur Nutzung von Office 365 an der Schule ist die Verarbeitung von personenbezogenen Daten erforderlich, die jedoch pseudonymisiert und datensparsam erfolgen. Die pseudonymisierten Anmeldedaten setzen sich aus den jeweils ersten beiden Buchstaben des Vor- und Nachnamens sowie einer willkürlichen Zahlenreihenfolge zusammen. Zu den personenbezogenen Daten gehören auch die Positionsdaten in Form einer Zahlenkombination, die die Gruppenzugehörigkeit abbilden soll.

Personenbezogene Daten der Benutzer von Office 365 werden erhoben, um dem Benutzer die genannten Dienste zur Verfügung zu stellen, die Sicherheit dieser Dienste und der verarbeiteten Daten aller Benutzer zu gewährleisten und im Falle von missbräuchlicher Nutzung oder der Begehung von Straftaten die Verursacher zu ermitteln und entsprechende rechtliche Schritte einzuleiten.

Die Verarbeitung personenbezogener Daten bei Nutzung von Office 365 erfolgt auf der Grundlage der DSGVO Art. 6 lit. a (Einwilligung).

Löschfristen

Mit dem Ende der Schulzugehörigkeit erlischt das Anrecht auf die Nutzung von Office 365. Entsprechend wird die Zuweisung von Office 365 Education-Lizenzen zu Benutzern mit Ende der Schulzugehörigkeit, in der Regel zum Schuljahresende, aufgehoben. Damit verliert der Benutzer den Zugriff auf Onlinedienste und -daten. Das bedeutet Folgendes:

- Alle Daten im Zusammenhang mit dem Konto dieses Benutzers werden von Microsoft 30 Tage aufbewahrt. Eine Ausnahme bilden Daten mit gesetzlicher Aufbewahrungspflicht, die entsprechend lange aufbewahrt werden.
- Nach Ablauf der 30-tägigen Frist werden die Daten von Microsoft gelöscht und können nicht wiederhergestellt werden. Ausgenommen sind Dokumente, die auf SharePoint Online-Websites gespeichert sind. Benutzer müssen ihre Daten vorher eigenständig sichern.

7. Einwilligung in die Nutzungsvereinbarungen für Schülerinnen und Schüler und die damit verbundene Verarbeitung personenbezogener Daten

Vollständiger Name des Schülers / der Schülerin:		
Geburtsdatum und Klasse:		

Kap. 2	Wir haben die Regeln zur Nutzung des **schuleignen Netzwerks und des WLAN** zur Kenntnis genommen (ab Klasse 7).
Kap. 3	Wir haben die Regeln zum **Umgang mit Iserv und die hiermit verbundene Datenverarbeitung** zur Kenntnis genommen.
Kap. 4	Wir haben die Regeln zum **Umgang mit mobilen Endgeräten** in der Schule zur Kenntnis genommen (ab Klasse 7).
Kap. 5	Wir haben die Regeln zum **MDM und die hiermit verbundene Datenverarbeitung** zur Kenntnis genommen (ab Klasse 7).
Kap. 6	Wir haben die Regeln zum Umgang mit **MS-Office** zur Kenntnis genommen.

Ort/Datum	**Unterschrift des Schülers/der Schülerin**
Ort/Datum	**Unterschrift des Erziehungsberechtigten**