

II. **Datenschutzerklärung - Personenbezogene Daten der Schüler, die im Zusammenhang mit IServ erhoben und gespeichert werden**

Gespeichert werden:

- Anmeldeinformationen in Form von Nutzerkennung (Kombination aus Vorname(n) und Nachname, das Passwort und die daraus resultierende IServ-eigene Emailadresse)
- Inhalte der Nutzer, wie zum Beispiel erstellte Dateien (Dokumente, Bilder, Videos) sowie ihre Versionen
- Daten, die vom Nutzer selbst erzeugt wurden sowie Gruppenmitgliedschaften in Klassen, Stufen sowie Kursen
- Zugriffsdaten in Form von Datum, Zeit, Gerät, IP-Nummern aufgesuchter Internetseiten und genutzter Dienste sowie der Traffic
- Kommunikationsdaten in Form von Empfänger und Absender von E-Mails und Messengerdiensten, Anzahl und Art der Dateianhänge sowie Datum- und Zeitstempel

Auf dem IServ am JHG werden folglich für die grundlegende Nutzung nur Vor- und Nachname sowie Klassen- und Stufenzugehörigkeit des Nutzers gespeichert, fast alle anderen Dateien werden vom Schüler/der Schülerin selbst erzeugt. Die im Hintergrund erzeugten Zugriffsdaten dienen dem Schutz vor und Nachverfolgung von möglichem Missbrauch.

Da sich die Schülerinnen und Schüler auch im schulinternen WLAN anmelden können, wird an dieser Stelle ebenfalls auf die dafür benötigten und gespeicherten Informationen hingewiesen:

- Nutzerdaten in Form der oben genannten Nutzerkennung
- Daten zur Geräteidentifikation in Form von Gerätenamen und MAC-Adressen (dies ist z.B. notwendig, um Schülerinnen und Schülern temporär den Zugang zum Internet am eigenen Endgerät zu gewähren)
- Die konkreten Zugriffsdaten auf das WLAN-Netzwerk (Datum, Zeit, genutzte Access-Points, Traffic und Ports)

Auswertung der Daten

Grundlegend werden die Daten lediglich dazu genutzt, den Schülerinnen und Schülern innerhalb des pädagogischen Netzwerks und des WLANs Dienste zur Verfügung zu stellen. Im Falle missbräuchlicher Nutzung oder gar der Begehung von Straftaten können anhand der oben angegebenen Daten Verursacher ermittelt werden und – je nach Ausmaß – schulinterne Konsequenzen oder rechtliche Schritte eingeleitet werden.

Die Daten werden - davon abgesehen - nicht eingesehen und anderweitig ausgewertet.

Weitergabe der Daten

In einigen Modulen werden im Fall der Nutzung zusätzliche Registrierungen/Anmeldungen notwendig. Hier bestehen aber Unterauftragsverarbeitungsverträge, es handelt sich also nicht um Dritte. Dies ist allerdings am JHG bisher nicht geplant.

Andere Übermittlungen finden ohne Einwilligung nicht statt.

Die IServ GmbH verarbeitet zudem auf Grundlage eines schriftlichen Vertrages als Auftragsverarbeiter weisungsgebunden personenbezogene Daten im Auftrag der Schule, allerdings zum Zwecke der Wartung des Schulservers IServ. Diese erfolgt als Fernwartung durch ausgewählte Mitarbeiter der IServ GmbH anhand einer Zwei-Faktor-Authentifizierung mit persönlichem SSH-Schlüssel und der weiteren Absicherung durch die App Duo Security. Zudem wird jeder Zugriff protokolliert und ist zudem einsehbar und überprüfbar.

Dateiübermittlungen an ein Drittland oder an eine internationale Organisation finden nicht statt und sind auch nicht geplant.

Der Server selbst steht in einem mit Türschloss gesicherten Raum in einem ebenfalls abgeschlossenen Serverschrank in der Schule, zu dem lediglich ein Administrator und wartungsbefugte Mitarbeiter der Gemeinde Senden Zugriff haben.

Einsichtsrechte in die gespeicherten personenbezogenen Daten

Die vom Nutzer selbst angelegten Daten, Kommunikationsinhalte und Dateien können direkt über die IServ-Oberfläche nach Anmeldung mit Nutznamen und Kennwort eingesehen werden. Sollte Bedarf bestehen, Zugriffsdaten für das pädagogische Netzwerk (z.B. Zeiten des Logins etc.) bzw. für das WLAN einzusehen oder sich die Inhalte des persönlichen Nutzerverzeichnisses aushändigen zu lassen, ist dies freilich möglich.

Dauer der Datenspeicherung

Zugangs- und Nutzungsdaten bleiben bestehen, solange die Schülerin/der Schüler Mitglied im pädagogischen Netzwerk ist. Bei Widerruf einer Einwilligung wird das Nutzerkonto gelöscht. Die Schülerinnen und Schüler haben die Möglichkeit, alle Daten zu löschen, auf die sie Schreibzugriff haben. Nach Ende der Schulzugehörigkeit werden die Zugangsdaten und das Nutzerverzeichnis gelöscht. Sicherheitshalber werden Konten und Gruppen allerdings noch für 90 Tage gespeichert und danach endgültig automatisch gelöscht. Videokonferenzen werden nicht gespeichert.

Logs selbst sind nicht änderbar, werden allerdings automatisch nach 6 Monaten gelöscht.

III. Nutzungsverordnung

Präambel

Die Schule stellt ihren Schülerinnen, Schülern und Lehrkräften (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 diesem Zugang erhält.

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 ein Dritter unberechtigt Kenntnis von seinem Passwort hat, so muss er sein Passwort unverzüglich ändern.

Sollte ein Nutzer sein Passwort vergessen haben, ist er verpflichtet, dieses 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.

Alle Nutzer sind verpflichtet, eingesetzte Filter und Sperren im pädagogischen Netzwerk 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 durch die Nutzer ist nicht zulässig, sie darf nur von den Administratoren durchgeführt werden. Dazu zählt auch die Erstellung von Skript-Dateien (z.B. Batch).

Administratoren

Die Administratoren haben weitere Rechte, verwenden diese aber grundsätzlich nicht dazu, sich Zugang zu persönlichen Konten bzw. persönlichen Daten zu verschaffen.

Protokolle

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

Hausaufgaben

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

In Phasen des Homeschoolings werden über IServ zudem Inhalte und Informationen bereitgestellt, die zur Bearbeitung der Aufgaben notwendig sind.

Verhaltensregeln zu einzelnen IServ-Modulen

Adressbuch

Die im gemeinsamen Adressbuch eingegebenen Daten sind für alle Nutzer sichtbar. Es wird deshalb geraten, so wenig personenbezogene Daten wie möglich von sich preiszugeben.

E-Mail

Soweit die Schule den Nutzern einen persönlichen E-Mail-Account zur Verfügung stellt, darf dieser nur für die schulische Kommunikation (interner Gebrauch) und damit ausschließlich für den Austausch von Informationen mit schulischem Zusammenhang 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 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.

In diesem Rahmen ist es ausdrücklich verboten, Informationen zu verschicken, die rechtlichen Grundsätzen widersprechen. Z.B. gilt dies für rassistische, ehrverletzende, beleidigende oder aus anderen Gründen gegen geltendes Recht verstoßende Nachrichten

Der gezielte oder willkürliche Versand von E-Mails im Rahmen von Massen-Mails bzw. Mailfluten (Spam) und Joke-Mails ist ebenso ausdrücklich verboten wie das Versenden von Mails mit anstößigen und unangemessenen Inhalten sowie solchen, die persönliche Rechte und Urheberrechte missachten oder verletzen.

Wer von missbräuchlichen Verwendungen von E-Mails (z.B. Cybermobbing, Spam) betroffen ist oder strafrechtlich relevante Inhalte zugeschickt bekommt, wendet sich an die Klassenlehrerin oder Klassenlehrer bzw. die Stufenleitung, damit unter Einbezug der Schulleitung weitere Schritte abgestimmt werden können.

Die Weiterleitung von E-Mails externer Anbieter (z.B. Gmail oder GMX) auf das IServ-Konto ist 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.

Eine neue Kommunikationsform bedeutet keine ständige Erreichbarkeit. Darauf müssen alle Beteiligten achten. Dazu gehören Respekt und Schutz von dienst- und unterrichtsfreien Zeiten. Dies kann gelingen, wenn alle Nutzer akzeptieren, dass ein Abrufen von Nachrichten durch den Empfänger in der Regel innerhalb von zwei Schultagen erfolgen soll („48-Stunden-Regel“). Dies betrifft Mitteilungen von allen Beteiligten untereinander (Schülerinnen und Schüler, Lehrkräfte sowie Schulleitung)

IV. Regelübersicht WLAN und BYOD

- Die Lehrkräfte entscheiden über die Benutzung/Verwendung der Geräte im Unterricht.
- Die Geräte werden nur für unterrichtliche Zwecke verwendet und die Lehrkräfte kontrollieren dies.
- Es werden keine unangemessenen/abgesprochenen Apps/Webseiten geöffnet.
- Fremde Geräte werden nicht genutzt.
- Wenn die Geräte verwendet werden, achten alle Schülerinnen und Schüler darauf, dass keine Sachschäden durch Unachtsamkeit entstehen.
- Es werden ohne Aufforderung der Lehrkraft keine Fotos/Videos von anderen gemacht.
- Während die Geräte in Verwendung sind, wird nicht getrunken.
- Passwörter werden nicht weitergegeben.
- Die Verwendung des schulischen WLAN-Netzes unterliegt den allgemein gültigen Nutzungsbedingungen der Schule.
- Das schulische WLAN-Netz ist eine schulische Ressource und darf somit nur für unterrichtliche Zwecke verwendet werden. Es versteht sich also von selbst, dass keine Social Media Seiten oder Messenger geöffnet werden oder das Netz außerschulisch verwendet wird.
- Die Schule haftet nicht für unsachgemäße/fahrlässige Verwendungen des Gerätes.
- Die Schule haftet nicht bei Diebstahl, Verlust oder Beschädigung des Gerätes, es besteht kein Versicherungsschutz.