BIRGER-FORELL-SEKUNDARSCHULE
BIRGER-FORELL-SEKUNDARSCHULE * Kantstr. 34 * 32339 Espelkamp

Einwilligung nach Art. 6 Datenschutz-Grundverordnung (DSVGO)

Nutzungsordnung & Datenschutzerklärung IServ

Präambel

Die Schule stellt ihren Schülerinnen und Schülern (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.

Datennutzung

Die Schule gleicht in regelmäßigen Abständen die Schülerdatenbank aus dem zentralen Schulverwaltungsprogramm für die Individualdaten- und Leistungsdatenverwaltung (SchilD) mit den IServ-Accounts der Schule ab. Aus Neuanmeldungen an der Schule wird ein IServ-Account generiert, wobei der Vor- und Zuname des Kindes mit der Domain-Endung: @birger-forell.de die Zugangsinformationen in Kombination mit einem erstmaligen Passwortvergabe-Code darstellen (Beispiel: vorname.nachname@birger-forell.de Rücksetzpasswort: 123456). Gemeinsam mit dem Vor- und Nachnamen wird auch die Jahrgangs- und Klassenzuordnung übermittelt. Accounts, die durch Schulabschluss oder -wechsel nicht mehr in der SchilD-Datenbank vorliegen, werden zur Löschung nach einer sechsmonatigen Karenzzeit angelegt.

Die so angelegten Accounts werden auf dem schuleigenen Server im hauseigenen Netzwerk abgelegt. Sie sind über die Seite: www.birger-forell.de aus dem internen Netzwerk, sowie extern aus dem Internet zugänglich.

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, 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. Lehrkräfte, Administratoren und betroffene Nutzer dürfen einen Rücksetzcode für einen Nutzer 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.

Protokolle

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

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.

Aufgaben (Wochenpläne, Vorbereitungsmaterial für Klassenarbeiten, etc.)

Aufgaben, wie Lernzeitwochenpläne, Übungen zur Klassenarbeitsvorbereitung, etc. können über IServ verbreitet werden, müssen aber im Unterricht angekündigt werden. Die Lehrkräfte achten dabei auf einen angemessenen Bearbeitungszeitraum.

Dateien

Die Schule stellt Nutzern einen Speicherbereich auf dem lokal gehostet IServ-Server für Dateien zur Verfügung, auf die über das Dateien-Modul auf der Website www.birger-forell.de oder der IServ-App zugegriffen werden kann. Zusätzlich ist es möglich einen WebDAV-Zugriff für verschiedene Betriebssysteme einzurichten, der die eigenen Dateien als Cloud-Ordner einbinden lässt. Der Zugang erfolgt in allen Fällen über die Authentifizierung mit den IServ-Anmeldedaten.

Der Nutzer verpflichtet sich, diesen Dateibereich nur für schulisch relevante Daten zu nutzen und insb. keine datenschutz- oder rechtsverletzenden Dateien abzulegen. Das wissentliche oder unwissentliche Ablegen von manipulierender oder schädlicher Software bzw. Dateien ist streng untersagt und kann zur Sperrung des Accounts sowie weiteren pädagogischen und strafrechtlichen Konsequenzen führen. Nutzer übernehmen in dem ihnen zumutbaren Rahmen die Verantwortung für die Einschätzung vertrauenswürdiger Download-Portale bzw. Internetseiten. Gleiches gilt für Dateien, die über einen externen Datenträger sowie einer WebDAV-Verbindung von einem privaten Gerät aufgespielt werden.

E-Mail

Soweit die Schule den Nutzern einen persönlichen E-Mail-Account zur Verfügung stellt, der auch eine Kommunikation mit Kommunikationspartnern außerhalb der Schule zulässt (interner und externer Gebrauch), ist folgendes zu beachten:

Der E-Mail-Account wird nur für den Austausch von Informationen im schulischen Zusammenhang bereitgestellt. Insbesondere darf der schulische E-Mail-Account nicht zur privaten Nutzung von Internetangeboten wie sozialen Netzwerken wie Facebook oder Twitter 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.

Private Kommunikation mit anderen Personen über diesen schulischen E-Mail-Account ist deshalb zu vermeiden, da nicht ausgeschlossen werden kann, dass die Inhalte von E-Mails Dritter durch Einsichtnahmen der Schule zur Kenntnis genommen werden.

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 eingeschränkten Nutzerkreis zur Verfügung, wie z.B. Gruppenforen. Darüber hinaus sind die Moderatoren der Foren (Lehrer) 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.

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. Auch kann die Nutzung des Messengers für Nutzer eingeschränkt werden.

Videokonferenzen im Rahmen des Unterrichts

Auf dieser Seite informieren wir Sie 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: Birger-Forell-Sekundarschule, Kantstr. 34, 32339 Espelkamp

Zu welchem Zweck sollen die Daten meines Kindes verarbeitet werden?

Die Verarbeitung ist erforderlich zur Nutzung des IServ-Videokonferenztools, einer Videokonferenz-Plattform, zur Durchführung von Online-Unterrichtseinheiten in der Lerngruppe und individueller Betreuung und Beratung in Kleingruppen oder Einzeltreffen zwischen Schüler und Lehrkraft.

Auf welcher Rechtsgrundlage erfolgt die Verarbeitung?

Die Verarbeitung erfolgt auf der Grundlage Ihrer Einwilligung.

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

Bei der Teilnahme an einer Videokonferenz werden neben Bild- und Tondaten, zusätzliche Daten zur Konferenz verarbeitet: Name des Raumes, IP-Adresse des Teilnehmers und Informationen zum genutzten Endgerät. Je nach Nutzung der Funktionen in einer Videokonferenz fallen Inhalte von Chats, gesetzter Status, Eingaben bei Umfragen, Beiträge zum geteilten Whiteboard, durch Upload geteilte Dateien und Inhalte von Bildschirmfreigaben an. Eine Speicherung von Videokonferenzen und Inhalten durch die Schule erfolgt nicht.

Wer hat Zugriff auf die personenbezogenen Daten meines Kindes?

Alle Teilnehmer einer Videokonferenz haben Zugriff im Sinne von Sehen, Hören und Lesen auf Inhalte der Videokonferenz, Chats, geteilte Dateien, Bildschirmfreigaben und Beiträge auf Whiteboards. Der Anbieter hat Zugriff auf die verarbeiteten Daten nur im Rahmen der Auftragsverarbeitung und auf Weisung der Schulleitung.

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, also weder für Werbung und auch nicht, um sie an Dritte weitergeben. Im Sinne des Datenschutzrechts findet somit keine Übermittlung statt.

Die Schule speichert keine personenbezogenen Daten im Zusammenhang mit der Nutzung des IServ-Videokonferenztools. Videokonferenzen und Chats werden nicht aufgezeichnet und weder durch Schule noch den Anbieter gespeichert. Die Inhalte von Chats, geteilte Dateien und Whiteboards werden in der Plattform gelöscht, sobald ein Konferenzraum geschlossen wird.

An die Server der IServ GmbH werden Klarnamen der Teilnehmer, IP-Adressen, Browserkennungen, Berechtigungen, Videokonferenz-Raum-Einstellungen wie beispielsweise der Raumname und die 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 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 Teilnehmer*innen 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.

Nutzung privater Endgeräte

Geltungsbereich

Die Nutzungsbedingungen gelten für die Nutzung der von den Eltern/ Erziehungsberechtigten erworbenen mobilen Endgeräte der Schülerinnen und Schüler.

Ausstattung

Die Eltern/ Erziehungsberechtigten erwerben über die Gesellschaft für digitale Bildung ein Bundle, das den jahrgangsspezifischen Anforderungen der Birger-Forell-Sekundarschule gerecht wird. Konkretere Informationen erhalten Sie bei der Schulanmeldung oder auf Nachfrage durch die Abteilungsleitung I bzw. den Schuladministratoren.

Zweckbestimmung der Nutzung der mobilen Endgeräte

Das mobile Endgerät wird von dem Nutzer in der Schule für schulische Zwecke genutzt.

Jeder Nutzer bringt sein eigenes mobiles Endgerät mit vollem Akku und ausreichender Speicherkapazität mit.

Für die Einhaltung der Zweckbestimmung der Nutzung ist die/der Erziehungsberechtigte bzw. sind die Erziehungsberechtigten zuständig.

Ansprüche, Schäden und Haftung

Das mobile Endgerät ist privates Eigentum und durch die im Bundle angebotene Versicherung umfassend versichert.

Schadens- und andere Versicherungsfälle klären die Eigentümer der mobilen Endgeräte direkt mit dem Anbieter, z.B. über das Smartsupport-Portal der Gesellschaft für digitale Bildung auf *www.dfgb.de/smartsupport*

Gehen der Verlust bzw. die Beschädigung auf eine dritte Person zurück, die nicht Vertragspartner ist, so sollte in Rücksprache mit der Schulleitung Anzeige bei der Polizei erstattet werden.

Nutzungsbedingungen

Beachtung geltender Rechtsvorschriften [Verhaltenspflichten]

Der Nutzer verpflichtet sich an die geltenden Rechtsvorschriften – auch innerschulischer Art – zu halten. Dazu gehören Urheber-, Jugendschutz-, Datenschutz- und Strafrecht sowie die Schulordnung.

Unabhängig von der gesetzlichen Zulässigkeit ist bei der Nutzung des mobilen Endgeräts nicht gestattet, verfassungsfeindliche, rassistische, gewaltverherrlichende oder pornografische Inhalte willentlich oder wissentlich abzurufen, zu speichern oder zu verbreiten.

Videos, Fotos oder Tonaufnahmen dürfen nur mit ausdrücklicher Erlaubnis der Lehrkraft und nach Zustimmung der aufgenommenen Personen erstellt werden und keinesfalls außerhalb des schulischen Rahmens gespeichert, weitergeleitet oder veröffentlicht werden (§ 201aStGB).

Besteht der Verdacht, dass das mobile Endgerät oder ein Computerprogramm/App von Schadsoftware befallen ist, muss dies unverzüglich der Schule gemeldet werden. Das mobile Endgerät darf im Falle des Verdachts auf Schadsoftwarebefall so lange nicht genutzt werden, bis die Schule die Nutzung wieder freigibt.

Zugriff auf das mobile Endgerät

Das mobile Endgerät darf nicht - auch nicht kurzfristig - an Dritte weitergegeben werden.

Eine kurzfristige Weitergabe an andere Schülerinnen und Schüler oder an Lehrkräfte ist erlaubt, soweit hierfür eine schulische Notwendigkeit besteht.

Im öffentlichen Raum darf die Ausstattung nicht unbeaufsichtigt sein.

Das mobile Endgerät ist in der ausgehändigten Schutzhülle aufzubewahren und darf aus dieser nicht entfernt werden. Die Hülle schützt das Gerät und fängt kleinere Stöße und Stürze ab.

Zugang zur Software des mobilen Endgeräts

Der Zugang zum Gerät soll mit einem Passwort gesichert werden.

Das Geräte-Passwort kann durch den schulischen Administrator zurückgesetzt, nicht aber eingesehen werden.

Grundkonfiguration zur Gerätesicherheit

Die Eigentümerin/ der Eigentümer gibt hiermit seine Einwilligung, dass das mobile Endgerät in das Mobile Device Management System der Birger-Forell-Sekundarschule eingepflegt und über dieses System hinsichtlich der schulischen Nutzung verwaltet wird.

Die Schule hat zur Filterung bestimmter illegaler, verfassungsfeindlicher, rassistischer, gewaltverherrlichender oder pornografischer Internetinhalte einen Contentfilter eingesetzt. Mittels dieses Contentfilters werden die Inhalte von Webseiten während des Browserbetriebs hinsichtlich einzelner Wörter, Phrasen, Bilder oder Links, die auf einen entsprechenden Inhalt hindeuten, automatisiert gefiltert und ggf. der Zugriff auf die Inhalte über das mobile Endgerät blockiert.

Die durch die Systemadministration getroffenen Sicherheitsvorkehrungen dürfen nicht verändert oder umgangen werden.

Damit automatische Updates auf ein Endgerät heruntergeladen und eingespielt werden können, muss das mobile Endgerät regelmäßig jeden zweiten Tag mit dem Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates müssen ausgeführt werden.

Die Verbindung zum Internet sollte nur über vertrauenswürdige Netzwerke erfolgen z. B. über das Netzwerk der Schule, das eigene WLAN zuhause oder einen Hotspot des eigenen Mobiltelefons. Bestehen Zweifel über die Sicherheit der zur Verfügung stehenden Netzwerke (z. B. im Café), sollte das Gerät nicht genutzt werden.

Im Unterricht muss die Nutzerin/ der Nutzer alle Benachrichtigungen deaktivieren, um Störungen zu vermeiden.

Datensicherheit (Speicherdienste)

Im schulischen Kontext dürfen Daten nur auf dem durch die Schule freigegebenen Dienst gespeichert oder ausgetauscht werden (IServ).

Alle schulischen Daten werden auf IServ gespeichert. Eine Datenspeicherung auf dem mobilen Endgerät soll vermieden werden, damit diese bei Verlust oder Reparatur nicht verloren gehen. Der Verleiher übernimmt keine Verantwortung für den Datenverlust, insbesondere auch nicht aufgrund von Gerätedefekten oder unsachgemäßer Handhabung.

Für die Sicherung der Daten ist ebenso die Nutzerin/ der Nutzer verantwortlich. Regelmäßige Backups sollten daher sichergestellt werden.

Technische Unterstützung

Die technische Unterstützung durch die Schule umfasst:

- die Grundkonfiguration des mobilen Endgerätes,
- eine Einweisung in die Grundkonfiguration des mobilen Endgerätes und dessen Nutzung,
- eine Checkliste zur Unterstützung bei der Gewährleistung einer sicheren Nutzung der mobilen Endgeräte.

Die Schule behält sich vor, jederzeit zentral gesteuerte Updates der auf den mobilen Endgeräten vorhandenen Software vorzunehmen, etwa um sicherheitsrelevante Lücken zu schließen.

Apps und sonstige Software mittels einer privaten Apple-ID werden auf eigene Verantwortung installiert. Die Schule übernimmt ausdrücklich weder die Haftung noch den Support für private Apps oder Anwendungen.

Zentrale Mobilgeräteverwaltung:

Das mobile Endgerät wird zentral mit Hilfe eines lokal gehosteten Relution-Servers und mit der Relution-Software über eine Mobilgeräteverwaltung administriert. Die Schule behält sich vor, über die Mobilgeräteverwaltung mobile Endgeräte wie folgt zu administrieren:

- Ersteinrichtung des Gerätes
- Übertragung von Nachrichten auf die Geräte
- Kamera an- und ausstellen
- Browser an- und ausstellen (Prüfungsmodus)
- Einzelanwendungsmodus
- Die Schule darf Profile erstellen, die Nutzungsbeschränkungen ermöglichen.

Voraussetzung für die Einrichtung des mobilen Endgerätes und die Mobilgeräteverwaltung durch die Schule ist die Verarbeitung der personenbezogenen Daten der Nutzerin oder des Nutzers. Dieser muss seine Einwilligung zur Verarbeitung personenbezogener Daten nach Artikel 7 Datenschutz-Grundverordnung geben. Bei Schülerinnen und Schülern unter 16 Jahren ist die Einwilligung der Erziehungsberechtigten erforderlich und erfolgt mit gesonderter Erklärung, die im nächsten Vertragspunkt aufgeschlüsselt wird. Die Einwilligungserklärung trägt insbesondere den Transparenz- und Informationspflichten nach Artikel 13 und Artikel 14 Datenschutz-Grundverordnung Rechnung.

Anerkennung der Nutzungsbedingungen

Ich versichere, die Nutzung des privaten mobilen Endgerätes in der Schule nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsbedingungen vorzunehmen.

Datenschutzerklärung „Relution“ (MDM)

Grundkonfiguration

Für das Mobile-Device-Management der privaten und schuleigenen iPads in unserem Schulsystem kommt ein Relution-Server zum Einsatz. Dieser ist im Schulgebäude hinter einer Firewall installiert und vor fremdem Zugriff geschützt. Beim Erwerb eines Endgeräts durch einen Anbieter, dessen Händlernummer in unserem System hinterlegt ist, wird die entsprechende Seriennummer des Gerätes dem Relution-Server übermittelt. Darüber erhält der Server Einblick in den allgemeinen Status des Geräts (Gerätename, Version des Betriebssystems, Speicherplatz, Akkustand) und Zugriff auf die Grundkonfiguration (Liste der Einstellmöglichkeiten im Anhang).

Für Endgeräte im Privatbesitz wird folgende Grundkonfiguration vorgenommen: Hinterlegung des schulischen WLAN-Passworts, Festlegen des Gerätenamens als ${user.name}, „Apple Classroom Einschränkungen von Apps und Geräten ohne Bestätigung erlauben“.

Schuleigene iPads erhalten diese und folgende Konfigurationen: „Relution“ & „IServ“-App erzwingen und dem Verbot folgender Punkte: Kopplung mit einer Watch, Booten in den

Wiederherstellungsmodus, Installation und Deinstallation von Apps, In-App-Käufe, App Store, Passwortänderung, Änderung des Gerätenamens, iCloud, Zurücksetzen auf Werkseinstellungen.

administrative Steuerung
Folgende Aktionen können durch den Systemadministrator über den Relution-Server auf allen iPads im Schulsystem durchgeführt werden: AirPlay Wiedergabe starten, AirPlay Wiedergabe stoppen, Alarm auslösen, App entfernen, App installieren, App vom Apple App Store installieren, Bildschirmzeit-Code entfernen, Gerät herunterfahren, Gerät neustarten, Gerät vollständig sperren, Geräteinformationen aktualisieren, Lost Mode aktivieren, Lost Mode deaktivieren, Nachricht senden, Passwort zurücksetzen, persönlichen Hotspot ein- oder ausschalten, Shortcut entfernen, Shortcut hinzufügen, Update Installieren. Der Systemadministrator der Birger-Forell-Sekundarschule verpflichtet sich, diese Aktionen auf privaten Endgeräten nur im ausdrücklichen Auftrag des Elternhauses durchzuführen (bspw. um vergessene Passwörter zurückzusetzen oder verlorene Geräte zu sperren und ggfs. zu orten).

Benutzerverwaltung
In der Geräteverwaltung des Relution-Servers wird eine LDAP-Verbindung zum IServ-Server der Birger-Forell-Sekundarschule aufgebaut. Dieser ist ebenfalls lokal im Schulgebäude installiert und bietet einen datenschutzkonformen Zugriff auf die dort gespeicherten Daten. Allen persönlich genutzten Endgeräten wird der jeweilige IServ-Account des Nutzers zugeordnet. Hierüber werden Vorname, Nachname und Gruppenzugehörigkeiten (Klassen, Jahrgang und Kurse) importiert. Durch die Anmeldung in der IServ-App auf dem iPad wird eine WebDAV-Verbindung zum eigenen Benutzerprofil auf dem IServ-Server aufgebaut. Dadurch steht die auf dem schulinternen IServ-Server gehostete persönliche Dateiablage als weiterer Speicherort dem Endgerät zur Verfügung.

Schülerinnen und Schüler können sich auf geteilten Endgeräten (stundenweise ausgegeben Klassensätzen) in der Relution-App mit ihrem IServ-Account authentifizieren und ebenfalls die persönliche Dateiablage nutzen. Alle lokal auf Geräten gespeicherten Daten werden nach der Abmeldung vom Gerät gelöscht.

Apple-Dienste und Appstore

Die Verwaltung durch den Relution-Server der Birger-Forell-Sekundarschule ermöglicht die Nutzung eines iPads ohne Apple-ID. Für den Unterricht benötigte Apps können durch die Grundkonfiguration, dem Aufspielen eines Unterrichtsprofils durch eine Lehrkraft oder dem Relution App-Store bezogen werden. Letzterer stellt einen schulinternen Appstore dar, der durch die Birger-Forell-Sekundarschule kuratiert wird, mit schulischen App-Lizenzen ausgestattet ist und eine Auswahl an Apps zum Download anbieten. Somit ist eine Nutzung gänzlich ohne Apple-Dienste möglich.

Alle darüber hinaus genutzten Apple-Dienste (bspw. Apple-ID, iCloud) können auf privaten Geräten in eigener Verantwortung genutzt werden. Das Erstellen einer Apple-ID stellt einen privaten Vertragsabschluss mit dem US-amerikanischen Unternehmen Apple dar und geschieht ohne jegliche Verantwortung der Birger-Forell-Sekundarschule. Zu keinem Zeitpunkt erfordert der schulische Gebrauch des iPads an der Birger-Forell-Sekundarschule die Nutzung oder das Erstellen einer Apple-ID.

Unterrichtsprofile

Die eindeutige Zuordnung der durch den Relution-Server verwalteten Endgeräte zu den entsprechenden IServ-Accounts ihrer Nutzer identifiziert Schülerinnen und Schüler als Mitglieder ihrer Klassen und Kurse. Ebenso sind alle dienstlichen Arbeitsgeräte der Lehrpersonen an der Birger-Forell-Sekundarschule ihren eindeutigen IServ-Accounts zugeordnet. Dies ermöglicht den Lehrkräften das Aufspielen zeitlich begrenzter Unterrichtsprofile auf den iPads ihrer Klassen und Kurse. Das Aufspielen eines Unterrichtsprofils blendet alle Apps und Einstellungen aus, die nicht ausdrücklich durch die Lehrperson erlaubt worden sind. Das Unterrichtsprofil wird durch das Stundenplanraster der Birger-Forell-Sekundarschule am Ende jeder Unterrichtsstunde automatisch beendet. Das Unterrichtsprofil sowie die ausgewählte Lerngruppe kann flexibel während der Laufzeit durch die Lehrperson angepasst werden.

verarbeitete Daten

Das MDM „Relution“ sieht folgende Informationen des Schüler-Tablets: IServ-Nutzername Gerätename, Seriennummer, Modellname und -nummer, Kapazität und freier Speicherplatz, iOS-Versionsnummer, installierte Apps, letzte Verbindung mit dem Relution-Server. Das MDM kann also insbesondere nicht auf die konkreten Daten zugreifen, wie beispielsweise E-Mails, Kalender, Kontakte, iMessages, Browser-Verlauf, FaceTime-Protokolle, Erinnerungen und Notizen, Fotos, Häufigkeit der Nutzung von Apps.
Das MDM kann ein Endgerät in den „Lost“-Modus versetzen, der die Ortung des Geräts ermöglicht. Der „Lost-Modus“ wird durch eine Sperrnachricht transparent auf dem Endgerät angezeigt, sodass eine Ortung ohne Kenntnis des Nutzers nicht möglich ist.

Nutzungsordnung „Apple Classroom“

Mit der Classroom App können Lehrkräfte iPad Geräte von Schülern im Unterricht verwalten und Schüler durch eine Unterrichtsstunde führen, indem sie Apps und Links für sie öffnen. Lehrkräfte können einfach Dokumente an alle in der Klasse senden und von ihnen empfangen und die Arbeit der Schüler auf ihrem Display im Blick behalten. Mit Classroom können die iPad Geräte der Schüler nur im Unterricht verwaltet werden und keine Daten werden nach dem Ende der Unterrichtsstunde gespeichert.

Dafür müssen die Lehrkraft und die Schüler in unmittelbarer Nähe zueinander, im gleichen WLAN angemeldet und in einer aktiven Unterrichtsstunde sein. Die Lehrkraft kann die Geräte der Schüler nicht außerhalb des Unterrichts verwalten oder einsehen. Um Transparenz bei der Verwendung der Bildschirmansicht für das Display eines Schülers im Unterricht sicherzustellen, zeigt eine Benachrichtigung am oberen Bildschirmrand an, dass der Bildschirm eingesehen wird.

Datenschutzerklärungen fachbezogener Apps

Anton

Anton ist eine Online-Plattform (App und Browser – https://anton.app/de/) mit Übungen in Mathe, Deutsch, Sachunterricht und Musik.

Zur Nutzung braucht jedes Kind ein persönliches Konto. In Anton werden dann die bearbeiteten Übungen und Lernerfolge festgehalten. Im Klassenkonto kann die Lehrkraft Ihres Kindes sehen, welche Übungen Ihr Kind bearbeitet hat und mit welchem Erfolg diese bearbeitet wurden. Bei Bedarf kann sie Ihrem Kind weitere passende Übungen zuweisen und Feedback geben. Auch Sie können mit Ihrem Kind sehen, wo es steht, wenn Sie sich gemeinsam einloggen.

Für die Nutzung von Anton ist es erforderlich, für jedes Kind ein passwortgeschütztes Nutzerkonto einzurichten. Dafür geben wir den Vornamen oder Spitznamen Ihres Kindes an.

Die Einwilligung ist freiwillig. Aus der Nichterteilung oder dem Widerruf der Einwilligung entstehen keine Nachteile. Die Teilnahme ist für Ihr Kind freiwillig. Im Falle einer Nichteinwilligung werden wir Ihrem Kind alternative Angebote zur individuellen Förderung bzw. während des Distanzlernens machen.
Die Einwilligung kann für die Zukunft jederzeit widerrufen werden. Im Falle des Widerrufs werden wir die entsprechenden Informationen mit dem Konto löschen. Soweit die Einwilligung nicht widerrufen wird, gilt sie für die Dauer der Schulzugehörigkeit, nach Ende der Schulzugehörigkeit werden die Daten gelöscht.
Gegenüber der Schule besteht ein Recht auf Auskunft Ihrer 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, der Landesbeauftragten für den Datenschutz und die Informationsfreiheit Nordrhein-Westfalen zu.

Canva

Es folgt die Zusammenfassung der Datenschutzrichtlinie der Canva Pty Ltd. Sie kann in ausführlicher Form unter https://www.canva.com/de_de/richtlinien/privacy-policy/ eingesehen werden. Gekürzt sind die jeweils die Verweisungen auf die Nutzung von Informationen Dritter für Angebote und Werbungen, da sie nicht für Schüler gelten, die Canva for Education nutzen. Laut eigener Datenschutzrichtlinie schaltet Canva keine Werbung für Schüler, die Canva for Education nutzen.

Hallo, hier ist unsere Richtlinie zum Datenschutz. In dieser Richtlinie wird dargelegt, wie Canva die Daten nutzt, die wir über dich sammeln, wenn du unseren Service nutzt. Diese Richtlinie informiert dich außerdem über deine Entscheidungsmöglichkeiten, wie wir deine Daten verwenden.

Wir sammeln Informationen über dich, die du uns freiwillig zur Verfügung stellst, z. B. wenn du ein Konto registrierst, den Service nutzt oder auf andere Weise mit uns interagierst.Wenn du unseren Service nutzt, z. B. wenn du dich über eine Anwendung eines Drittanbieters einloggst, können wir von dieser Anwendung Informationen über dich erhalten.Wir sammeln automatisch bestimmte Informationen darüber, wie du unseren Service nutzt. Weitere Informationen darüber, wie wir diese Informationen von dir sammeln, findest du in unserer Cookie-Richtlinie.

Wir senden Cookies an deinen Browser, um dir die Nutzung von Canva zu erleichtern. Immer wenn du eine Canva-Seite aufrufst, sendet dein Browser Informationen über sich selbst und deine Interaktion mit unserem Service. Diese Informationen werden auf unseren Servern gespeichert. Wir können kleine Bilder verwenden, um zu überprüfen, wie viele Menschen unsere E-Mails öffnen und unsere Website besuchen.

Dein Telefon oder Gerät sendet uns Informationen über deine Nutzung. Canva kann deine Standortdaten für Personalisierung, Analysen und steuerliche Zwecke erfassen und nutzen. Canva sammelt die Inhalte, die du in dein Konto hochlädst.

Canva verwendet Informationen über dich aus verschiedenen Gründen, unter anderem um den Dienst bereitzustellen, anzupassen und zu verbessern. Möglicherweise teilen wir einige Informationen über

dich mit unseren Geschäftspartnern und Drittanbietern, um dir den Service zur Verfügung zu stellen oder um die berechtigten Geschäftsinteressen von Canva zu erfüllen.

Unsere Designs sind standardmäßig privat. Wenn du Designs teilst, achte auf angemessene Privatsphäre-Einstellungen. Für Designs mit persönlichen oder vertraulichen Informationen raten wir von der Einstellung „Alle mit dem Link“ ab.

Wenn wir unser Unternehmen verkaufen, können alle Informationen, die wir über dich gesammelt haben, Teil des Verkaufs sein. Wir können bestimmte Informationen an deinen Arbeitgeber weitergeben. Wir können deine Daten weitergeben, wenn du deine Nutzung von Canva mit Anwendungen von Drittanbietern integriert hast, die nicht von uns kontrolliert werden.

Wir können anonymisierte Daten an Dritte weitergeben. Wir können Daten gemäß unserer Richtlinie für Behördenanfragen oder wenn wir es für notwendig halten an Behörden weitergeben.

Um unseren Service zu betreiben, haben wir Canva-Gruppenmitglieder und Verkäufer auf der ganzen Welt. Das bedeutet, dass deine Daten in die USA, nach Australien, Europa, Singapur, auf die Philippinen, nach Neuseeland und an jeden anderen Ort, an dem der Service betrieben wird, übertragen werden können. Wir möchten deine Daten sicher aufbewahren und haben branchenweit anerkannte Maßnahmen ergriffen, um sie zu schützen. Absolute Datensicherheit können wir allerdings nicht garantieren.

Du hast die Kontrolle über deine Kontoeinstellungen, wie z. B. deine Kontoinformationen und Marketing-E-Mail-Benachrichtigungen, aber es gibt ein paar wichtige Dinge, die wir dir immer schicken. Wenn du Fragen zur Überprüfung oder Änderung deiner Kontoinformationen hast, kannst du uns über privacy@canva.com. direkt kontaktieren.

Wenn wir keine Informationen über dich sammeln sollen, kannst du möglicherweise entsprechende Änderungen an den Einstellungen in deinem Browser oder Gerät vornehmen. Du kannst den Erhalt von Canva-Werbeaktionen ablehnen, die auf Informationen von Dritten über dich basieren, zum Beispiel deine Berufsbezeichnung und deinen Arbeitgeber. Je nachdem, wo du wohnst, hast du möglicherweise bestimmte Rechte in Bezug auf deine Daten. Canva bietet dir in den Einstellungen deines Kontos eine Reihe von Kontrollmöglichkeiten und du kannst deine Datenschutzrechte per E-Mail an privacy@canva.com einsehen.

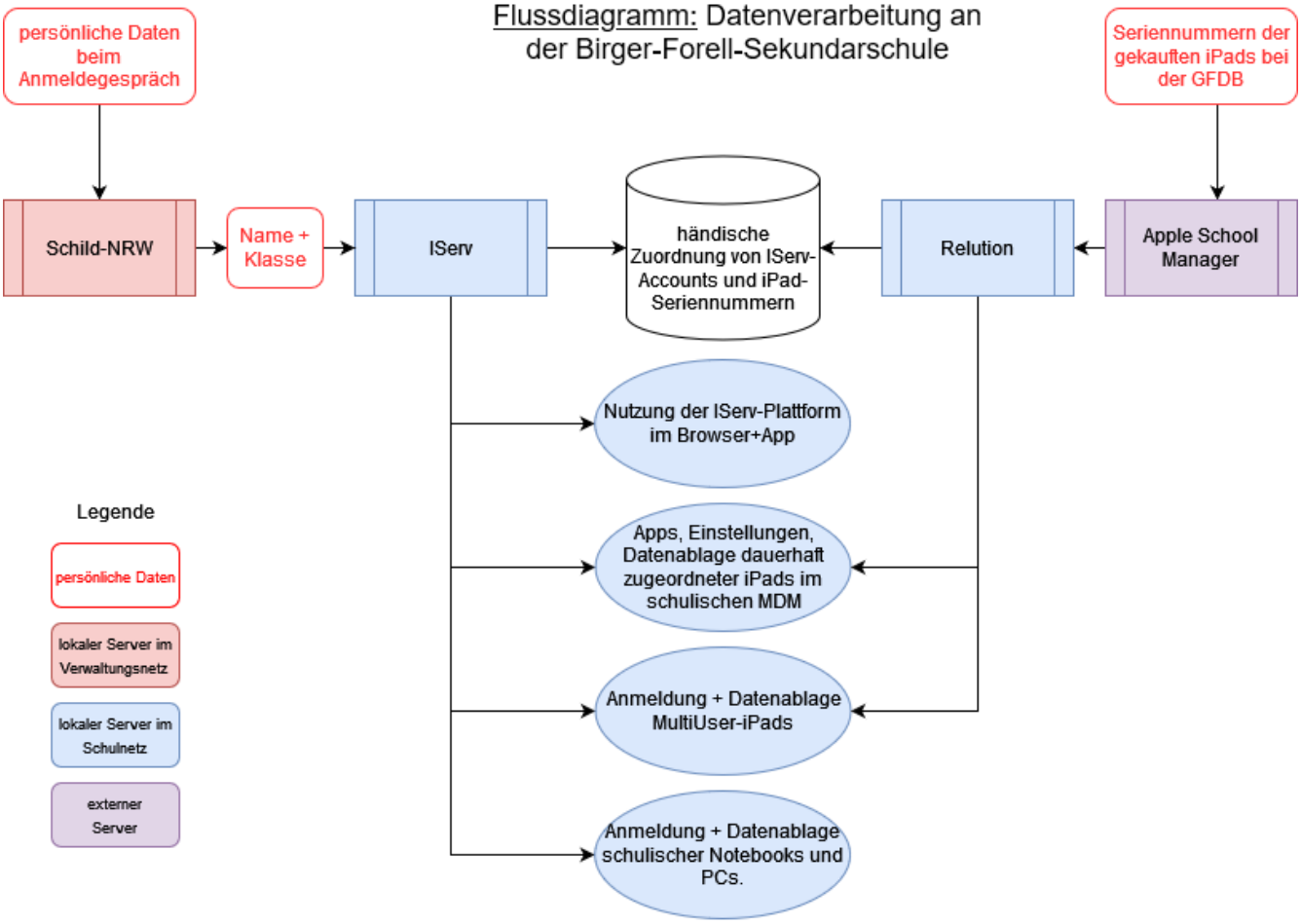
Wir speichern Ihre Profilinformationen und Benutzerinhalte, um Ihnen unseren Service zur Verfügung stellen zu können und um unseren gesetzlichen und behördlichen Verpflichtungen nachzukommen.

Wir haben einen sicheren Raum für Kinder geschaffen, in dem sie unter Aufsicht von Lehrkräften Canva nutzen können. Unser Hauptdienst auf canva.com ist nicht für Kinder gedacht.

Wenn wir auf Canva einen Link zu einer Website eines Dritten anbieten, können wir nicht kontrollieren, was am anderen Ende passiert. Das Gleiche gilt, wenn du deine Daten auf Canva einer anderen Website zur Verfügung stellst; die Verwendung deiner Daten unterliegt den Datenschutzrichtlinien des Drittanbieters.

Wenn du von Europa aus auf unseren Dienst zugreifst, ist Canva Pty Ltd. der Verantwortliche für deine personenbezogenen Daten. In einigen Fällen verarbeiten wir deine Daten jedoch nur im Namen eines Teams als Verarbeiter. Wir verarbeiten deine Daten nur, wenn wir eine rechtmäßige Grundlage haben. Wir können deine Daten vorbehaltlich angemessener Sicherheitsvorkehrungen außerhalb Europas übertragen.

Anlage


Flussdiagramm: Datenverarbeitung an der Birger-Forell-Sekundarschule
persönliche Daten beim Anmeldegespräch
Seriennummern der gekauften iPads bei der GFDB
Schild-NRW
Name + Klasse
IServ
händische Zuordnung von IServ-Accounts und iPad-Seriennummern
Relution
Apple School Manager
Nutzung der IServ-Plattform im Browser+App
Apps, Einstellungen, Datenablage dauerhaft zugeordneter iPads im schulischen MDM
Anmeldung + Datenablage MultiUser-iPads
Anmeldung + Datenablage schulischer Notebooks und PCs.
Legende
persönliche Daten
lokaler Server im Verwaltungsnetz
lokaler Server im Schulnetz
externer Server