

IServ Nutzungsordnung der Dietrich-Bonhoeffer-Schule

1. Präambel

Die Dietrich-Bonhoeffer-Schule (im Folgenden: Schule) stellt ihren Schüler*innen und Lehrkräften (im Folgenden: Nutzer*innen) als Kommunikations- und Austauschplattform IServ zur Verfügung. Diese Plattform kann mit einem eigenen Zugang sowohl über die PCs im lokalen Schulnetzwerk als auch von jedem Computer bzw. Handy mit Internetzugang außerhalb der Schule genutzt werden. IServ ist eine digitale Schulplattform, die der schulischen Kommunikation und Zusammenarbeit dient und allen Nutzern ermöglicht, schulbezogene Daten zu speichern und auszutauschen. Darüber erfolgt die Nutzung der schulischen digitalen Endgeräte über die Anmeldung im lokalen Schulnetzwerk, welches durch den schulinternen IServ-Server organisiert wird. Die Daten der webbasierten Plattform und die des lokalen Schulnetzwerks werden schulintern auf einem Server gesichert. Um IServ nutzen zu können, ist eine Einwilligung des Nutzers bzw. der Nutzerin / der Erziehungsberechtigten notwendig.

Die IServ-Schulplattform und die Nutzung der schulinternen digitalen Endgeräte der Dietrich-Bonhoeffer-Schule ist nur für Mitglieder der Schule mit einer Registrierung zugänglich. Alle Nutzer*innen verpflichten sich, die Rechte anderer Personen zu achten und die verbindlichen Regeln der vorliegenden Nutzungsordnungen einzuhalten. Eine Weitergabe der Zugangsdaten an Dritte, d.h. schulfremde Personen der DBS, ist nicht erlaubt.

2. Nutzung von IServ an der Dietrich-Bonhoeffer Schule

2.1 Nutzung der webbasierten Plattform IServ

Die IServ-Plattform der Dietrich-Bonhoeffer-Schule ist für alle registrierten Nutzer*innen über die Internet-Adresse <https://bonhoeffer-schule-re.schulserver.de/iserv/> erreichbar.

Auf der Plattform werden verschiedene Module zur Kommunikation verwendet. Die Schule entscheidet darüber, welche IServ-Module wann für den innerschulischen Gebrauch freigeschaltet werden und welcher Nutzerkreis zu diesem Zugang erhält. Die Module der IServ-Plattform dürfen ausschließlich zur schulischen Kommunikation und Arbeit der Nutzer*innen verwendet werden.

Die Schule übernimmt keine Verantwortung für die Inhalte und die Art gespeicherter Daten. Die Sicherung eigener in IServ (webbasiert) gespeicherter Dateien im Dateien-, Messenger, Foren- oder im E-Mail Modul gegen Verlust obliegt der Verantwortung der Nutzer. Die Verhaltensregeln für die webbasierte IServ-Plattform werden ab Kapitel 5 erläutert.

2.2 Nutzung des lokalen Schulnetzwerks in der Schule

Die Verwendung der schuleigenen digitalen Endgeräte am Schulort (Hunsrückstraße 15, 45665 Recklinghausen) und die damit verbundene Anmeldung im lokalen Schulnetzwerk erfolgt über die IServ-Zugangsdaten. Die IServ-Oberfläche sollte an den eingebundenen Schulrechnern immer über den Menüpunkt ‚Abmelden‘ verlassen werden, da ansonsten andere auf deine eigenen Daten zugreifen können.

Die Arbeit an den digitalen Endgeräten ist nur für schulische Zwecke und nach Genehmigung durch eine Lehrkraft gestattet. Speichern von digitalen Inhalten ist nur durch Aufforderung von Lehrkräften gestattet. Die Sicherung der Daten erfolgt in der Regel auf der webbasierten Plattform. Dateien werden nach Ende des Schuljahres gelöscht.

Das Senden, Aufrufen und Speichern jugendgefährdender und anderer strafrechtlich relevanter Inhalte ist auf der Schulplattform und der Server ebenso verboten wie die Speicherung von URLs (Webseiten) oder Links auf jugendgefährdende Websites oder Websites mit strafrechtlich relevanten Inhalten.

Weil umfangreiche Up- und Downloads die Arbeitsgeschwindigkeit des Servers beeinträchtigen und darüber hinaus schädlich sein können, 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. Verstöße dagegen können schulrechtliche Konsequenzen mit sich ziehen. Die Ahndung von Verstößen liegt im Ermessen der Schulleitung.

2.3 Nutzungsregelung für den Wlan-Zugang und Internetnutzung an der DBS

Die Schule eröffnet seinen Schülerinnen und Schülern im Bereich des Schulgeländes als freiwilliges Angebot kostenlos den Zugang zum Internet über ein WLAN, wenn die folgenden Regelungen anerkannt werden. Das freiwillige Angebot der Internet-Nutzungsmöglichkeit kann individuell oder generell durch die Schule eingeschränkt werden.

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

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.

Es ist untersagt die IServ Zugangsdaten Dritten zugänglich zu machen, um die Nutzung des Wlans zu ermöglichen. Im Zweifelsfall haftet der registrierte Nutzer/die registrierte Nutzerin für unzulässige Aktivitäten Dritter bei der Nutzung seines/ihres WLAN-Zugangs.

Nutzungseinschränkungen durch das Vorhandensein von Jugendschutzfiltersoftware der Schule sind zu akzeptieren. Der Versuch, die technischen Filtersperren zu umgehen, kann zum Entzug der Nutzungserlaubnis führen.

Die Schule übernimmt keine Haftung für die Datensicherheit der von den Nutzer*innen genutzten privaten Geräte. Die Verantwortung hierfür liegt ausschließlich bei den Nutzerinnen und Nutzern. Ein Manipulationsversuch an der Netzinfrastruktur kann zivil- und strafrechtlich verfolgt werden, sowie schulinterne Konsequenzen mit sich tragen.

Die Nutzungsaktivitäten der Nutzer*innen werden personenbezogen protokolliert und gespeichert. Diese können im Fall der missbräuchlichen Nutzung des Zugangs von der Schule oder einem von ihr beauftragten Dienstleister ausgewertet oder personenbezogen an Strafverfolgungsbehörden übermittelt werden. 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.

Die Einwilligung der Nutzungsregelung erfolgt mit der Unterschrift zur Erstellung eines IServ-Kontos. Der Widerruf der Einwilligungserklärung kann ohne die Angabe von Gründen jederzeit erfolgen.

3. Der IServ-Zugang („Account“)

Für den Zugang zu der IServ-Plattform und des lokalen Schulnetzwerks der Dietrich-Bonhoeffer Schule ist ein individuelles Nutzerkonto bzw. Account erforderlich. Jedes Mitglied der Dietrich-Bonhoeffer-Schule kann einen solchen persönlichen Account erhalten. Die Accounts der Schüler*innen werden in der Regel zu Beginn des Schuljahres generiert.

Um einen Account zu erstellen, werden der Vor- und Nachname sowie eine von der Schule zugewiesene Identifikationsnummer an den IT-Dienstleister der Stadt Recklinghausen, die GKD, weitergegeben. Von

dort aus werden die Accounts der Schüler*innen erstellt. Dabei wird aus dem Anfangsbuchstaben des Vornamens und des Nachnamens ein Benutzername angelegt (m.mustermann). In Einzelfällen werden die Accounts und Zugangsdaten durch die IServ-Administratoren der Schule erstellt. Der Benutzername mit einem vorläufigen Passwort wird dann über die Schule an die Nutzer*innen weitergeleitet. Bei jeder Anmeldung bei der IServ-Schulplattform werden die IP-Nummer des Nutzers bzw. der Nutzerin und die Art und Weise des Logins gespeichert.

4. Passwörter

Bei der ersten Anmeldung kann nach Eingabe des Benutzernamens (bei IServ „Account“ genannt) und des vorläufigen Passworts ein individuelles Passwort gesetzt werden.

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 Nutzer*innen mitzuteilen. Erfährt ein/e Nutzer*in, dass ein Dritter unberechtigt Kenntnis von seinem Passwort hat, so muss er sein/ihr Passwort unverzüglich ändern.

Sollte ein/e Nutzer*in das Passwort vergessen haben, ist er/sie verpflichtet, dass durch Lehrer*innen oder Administratoren neu vergebene Passwort beim nächsten Einloggen sofort zu ändern. Hierfür muss sich der/die Nutzer*in eigenständig und zeitnah bei einem Lehrer / einer Lehrerin bzw. einem Administrator melden, damit das Passwort zurückgesetzt werden kann. Nur ein/e Nutzer*in selbst darf ein neues Passwort für sich persönlich beantragen. Darüber hinaus sind alle Nutzer*innen verpflichtet, eingesetzte Filter und Sperren zu respektieren und diese nicht zu umgehen.

5. Allgemeine Verhaltensregeln

Im Sinne des Leitziels der Dietrich-Bonhoeffer-Schule „erfolgreiches Lernen und sozial handeln“ werden folgende Regeln formuliert, die in der Kommunikation in allen Modulen auf der IServ-Schulplattform gelten. Im Anschluss werden zusätzliche Verhaltensregeln zu den einzelnen IServ-Modulen erläutert.

5.1 Kommunikationsregeln

Für die auf der IServ-Plattform zur Verfügung gestellten Chat-Rooms, Foren und E-Mail-Austausch gelten folgende Regeln:

- Alle Benutzer*innen verpflichten sich zu einer respektvollen Kommunikation miteinander.
- Verboten sind rassistische, pornographische oder Gewalt verherrlichende Äußerungen oder Bilder / Videos.
- Die Verwendung irreführender Nicknames ist untersagt.
- Die Kommunikation ist angemessen und sachlich.
- Ganze Wörter oder Sätze in Großbuchstaben stehen auf IServ für lautes Schreien. Das ist unhöflich und an unserer Schule nicht erwünscht.
- Das Gleiche gilt für das endlose Wiederholen von Wörtern, Sätzen, URLs oder sinnloser Zeichenfolgen.
- Persönliche Beleidigungen bzw. private Streitereien und Auseinandersetzungen haben nichts auf IServ zu suchen und werden geahndet.

6. Protokolle

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

7. Verhaltensregeln zu den einzelnen IServ-Modulen

7.1 Adressbuch

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

7.2 Aufgaben

Das Aufgaben-Modul wird für das Verteilen und Bearbeiten von Aufgaben im Rahmen des Regelunterrichts und Distanzunterrichts verwendet. Die Lehrkräfte stellen in dem Modul Aufgaben, die die Schüler*innen im geforderten Format „Bestätigung“, „Text“ und/oder „Hochladen einer Datei“ bearbeiten müssen. Der Schüler / die Schülerin ist verpflichtet diese Aufgaben im geforderten Bearbeitungszeitraum zu bearbeiten und auf dem IServ Schulserver digital abzugeben. Hierbei bestätigen die Schüler*innen, dass die eingereichten Lösungen eigenständig erstellt wurden. Das Einreichen von Aufgabenlösungen bzw. das Hochladen von Dokumenten anderer Personen ist nicht gestattet.

Die eingereichten Lösungen werden nach den Bewertungsrichtlinien des jeweiligen Faches bewertet und fließen in die Gesamtbewertungen des Schülers / der Schülerin ein.

7.3 Dateien

Jede/r Nutzer*in erhält im Dateien-Modul einen Bereich, der zum Speichern von unterrichtsbezogenen Dateien genutzt werden kann. Eine anderweitige Nutzung ist nicht gestattet.

Im Dateien-Modul wird grundsätzlich zwischen einer eigenen Dateien-Ablage „Eigene“ und Gruppenordnern „Gruppe“ unterschieden. Während die „Eigene“-Ablage nur von dem Nutzer / der Nutzerin selbst verwendet und nicht von anderen Nutzer*innen einsichtbar ist, ist die „Gruppen“-Ablage von allen Mitgliedern einer gemeinsamen Gruppe gleichberechtigt nutzbar. Eine so-genannte „IServ-Gruppe“ wird aus bestimmten Nutzer*innen gebildet, die Gemeinsamkeiten besitzen (z.B. Klassen- und Kurszugehörigkeiten, AGs, SV, usw.).

7.4 E-Mail

Alle Nutzer*innen besitzt eine persönliche E-Mail-Adresse, die aus dem Account-Namen und dem Namen des Schulservers (@bonhoeffer-schule-re.schulserver.de) besteht. Diese darf nur für die schulische Kommunikation (internen Gebrauch) verwendet werden. Ein Versenden von E-Mails ist für Schüler*innen nur an Nutzer*innen des schulinternen IServ Schulservers möglich. Die Schule ist damit kein Anbieter von Telekommunikation im Sinne von § 3 Nr. 6 Telekommunikationsgesetz. Ein Rechtsanspruch der Nutzer*innen 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 schulische E-Mail-Adresse darf nicht zur Anmeldung bei Internetadressen jeglicher Art verwendet werden. Das gilt insbesondere für alle sozialen Netzwerke (Facebook, Instagram,...).

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*innen werden hierüber unverzüglich informiert.

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

7.5 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, wie z.B. Gruppenforen. Darüber hinaus sind die Moderatoren der Foren berechtigt, unangemessene Beiträge zu löschen oder zu bearbeiten. Moderatoren dürfen nur in dem ihnen anvertrauten Foren moderieren. Von „außen“, d.h. für nichtregistrierte IServ-Benutzer*innen sind diese Bereiche nicht zugänglich.

7.6 Kalender

Kalendereinträge für Gruppen werden nach bestem Wissen eingetragen und nicht manipuliert. Es besteht kein Anspruch auf Vollständigkeit.

7.7 Messenger

Es gelten die gleichen Vorgaben wie bei der E-Mail-Nutzung und insbesondere die Kommunikationsregeln (siehe 5.1).

7.8 Texte, Tafeln und Office

Die Module Texte, Tafeln und Office dürfen nur zur Bearbeitung und Organisation von schulischen Aufgaben verwendet werden. Da es sich hierbei um Module handelt, die unter anderem gemeinschaftlich mit anderen Nutzer*innen genutzt werden, gelten die gleichen Vorgaben wie bei der E-Mail-Nutzung und insbesondere die Kommunikationsregeln (siehe 5.1). Die angefertigten und gespeicherten Ergebnisse bzw. Werke in den Modulen müssen von dem Nutzer und der Nutzerin eigenständig erstellt worden sein. Die Verwendung von Werken anderer Personen ist nicht gestattet.

8. Nutzungsordnung des Videokonferenz-Moduls

8.1 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. Eine eigene Einwilligung ist für die Nutzungsordnung des Videokonferenz-Moduls notwendig.

8.2 Videokonferenzen

8.2.1 Zugangsdaten

An einer Webkonferenz dürfen nur berechtigte Personen teilnehmen, die einen Zugang für die Schulplattform IServ besitzen.

8.2.2 Daten, die im Rahmen einer Videokonferenz 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.

8.2.3 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.

8.3 Regeln für Videokonferenzen

- Bei Webkonferenzen und im Distanzunterricht 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.
- Es ist generell untersagt, dass ein Dritter (auch Eltern, Freunde, Geschwister usw.) beim Distanzunterricht zuhören, zusehen oder sonst wie einen Einblick in die Kommunikation erhalten.
- Der persönliche Account für den Zugang zur Webkonferenz bzw. zum Distanzunterricht darf an keine andere Person weitergegeben werden.
- Die Nutzung des Videokonferenzmoduls in öffentlich zugänglichen Räumen wie z.B. Cafés, Kneipen, Restaurants, ÖPNV, Warteräume, Arztpraxen, Läden usw. ist nicht gestattet.

Hinweis: Wählen Sie einen passenden Ort für die Videokonferenz, wenn Bild- und Tonübermittlung aktiviert sind, da die anderen Konferenzteilnehmer*innen ihr privates Umfeld im Hintergrund sehen können. Ideal ist eine aufgeräumte Arbeitsumgebung mit unaufgeregtem Hintergrund oder eine weiße Wand.

8.4 Kommunikations- und Verhaltensregeln während Videokonferenzen

- Die Nutzer*innen sind verpflichtet beim Betreten des Videokonferenzraum auf die Frage „Wie möchten Sie der Konferenz beitreten?“ mit der Auswahl der Funktion „mit Mikrofon“ zu antworten. Die Einstellung „nur zuhören“ erlaubt es den Nutzer*innen nicht sich per „Sprechen“ an der Videokonferenz zu beteiligen, sodass eine aktive Teilnahme an der Videokonferenz (im Regelfall: Unterricht) nicht gegeben ist. Das Mikrofon ist nicht automatisch auf „laut“ geschaltet, sondern kann individuell „entstummt“ werden.
- Der „persönliche Echotest“ muss durchgeführt werden, da dabei die Funktion des Mikrofons überprüft wird. Der Echotest kann nur vom jeweiligen Nutzer / der Nutzerin gehört werden.
- Nach Betreten des Videokonferenzraums schaltet die / der Nutzer*in das Mikrofon sofort stumm, um die Konferenz mit individuellen Nebengeräuschen nicht zu stören.
- Darüber hinaus gilt: Wer nicht spricht, schaltet sein Mikrofon stumm!
- Bei Betreten der Videokonferenz ist die Kamerafunktion ausgeschaltet. Achten Sie jedoch darauf, dass Sie die Kamerafunktion nicht aus Versehen betätigen.
- Die Lehrkraft entscheidet darüber, ob die Kamerafunktion in der Videokonferenz eingeschaltet werden darf.
- Ist die Kamerafunktion erlaubt, so muss der Nutzer / die Nutzerin das Kamerabild - wenn möglich - klein schalten.
- Der „Öffentliche Chat“, „private Chat“ und die „geteilten Notizen“ werden nur für schulische Nachrichten verwendet. Ein privater Austausch von Nachrichten zwischen Nutzer*innen ist nicht gestattet.
- Auch wenn die Webkonferenz am Computer stattfindet, sind „Nebenbeschäftigungen“ wie Tippen auf der Tastatur oder Herumklicken in verschiedenen Fenstern - vor allem bei aktiviertem Mikrofon verboten. Wenn Ihr Betriebssystem einen Nicht-Stören-Modus hat, schalten Sie ihn ein.

9. Datenschutzrechtliche Information (Art. 12 DS-GVO) zum IServ Videokonferenztool

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

9.1 Wer ist verantwortlich für die Verarbeitung der Daten meines Kindes?

Verantwortlich ist die Schule:

Dietrich-Bonhoeffer-Schule
Hunsrückstraße 15
45665 Recklinghausen

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

Fragen zum Datenschutz können Sie an den behördlich bestellten schulischen Datenschutzbeauftragten stellen: Dr. N. Koschwitz: nkoschwitz@bonhoeff.schulen-re.de

9.3 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.

9.4 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.

9.5 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 personenbezogen 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.

9.6 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.

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

Unsere Videokonferenz-Instanz wird von IServ für die Schule 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.

10. Löschung des IServ-Accounts

Der IServ Account wird mit Beendigung des Schulverhältnisses gelöscht. Die Nutzer*innen sind verpflichtet persönliche Dokumente im Vorhinein separat zu sichern. Eine Sicherung durch die Schule ist nicht gegeben.

11. Änderungen der Nutzungsordnung

Änderungen der Nutzungsordnungen werden den Erziehungsberechtigten schriftlich im Rahmen eines Elternbriefes mitgeteilt. Sollten Teile der vorherstehenden Regeln unwirksam werden, bleiben die übrigen in Kraft.

12. Verstöße

Im Fall von Verstößen gegen die Nutzungsordnung kann das Konto temporär oder permanent gesperrt werden. Damit ist 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 Schulleitung.