IT
und
Datenschutz

Nutzungsordnung der IT-Systeme, des WLAN-Netzes und des Internets an der Bischöflichen St. Angela-Schule Düren für Schülerinnen und Schüler

A. Allgemeines

Die Bischöfliche St. Angela-Schule Düren gibt sich für die Benutzung von schulischen Computereinrichtungen mit Internetzugang, Messengerdiensten und Videokonferenzsoftware sowie des WLAN-Netzes der Schule die folgende Nutzungsordnung. Diese gilt für die Nutzung von Computern und des Internets durch Schülerinnen und Schüler im Rahmen des Unterrichts, der Gremienarbeit sowie außerhalb des Unterrichts zu unterrichtlichen Zwecken. Darüber hinaus verpflichten sich alle Mitglieder der Schulgemeinschaft zur Beachtung der Digiquette.

Die Information zur Verarbeitung personenbezogener Daten an der Bischöfliche St. Angela-Schule Düren finden Sie unter folgendem Link: https://angela-dueren.de/informationen-zum-datenschutz/

B. Regeln für jede Nutzung

1. Schutz der Geräte

Die Bedienung der schuleigenen Hard- und Software erfolgt entsprechend den vorhandenen Instruktionen. Störungen oder Schäden sind unbedingt sofort der aufsichtführenden Person zu melden. Wer schuldhaft Schäden verursacht, hat diese zu ersetzen. Bei Schülerinnen und Schülern, die das 18. Lebensjahr noch nicht vollendet haben, hängt die Verantwortlichkeit von der für die Erkenntnis der Verantwortlichkeit erforderlichen Einsicht ab (§ 828 (3) i.V.m. 823 BGB). Nachdem elektronische Geräte durch Schmutz und Flüssigkeiten besonders gefährdet sind, sind während der Nutzung der Computer und Tablets, Essen und Trinken verboten.

2. Anmeldung an den Computern, Videokonferenzen und dem WLAN der Schule

Zur Nutzung ist eine Authentifizierung mit Benutzernamen und einem Passwort erforderlich. Nach Beendigung der Nutzung melden sich die Schülerin oder der Schüler am PC bzw. beim benutzten Dienst ab. Für Handlungen im Rahmen der schulischen Internetnutzung sind die jeweiligen Schülerinnen und Schüler verantwortlich. Insbesondere das WLAN der Schule verlangt eine maßvolle Nutzung. **Die Nutzung des Wlans ist nur für unterrichtliche Zwecke erlaubt, d.h. das Herunterladen von privaten Apps, das Spielen von nicht unterrichtsrelevanten Computerspielen, etc. sind untersagt.**

Das Passwort muss vertraulich behandelt werden. Die Verwendung falscher Namen bzw. das Arbeiten unter einem fremden Passwort ist nicht gestattet. Das Passwort muss allgemeinen Sicherheitsstandards genügen, das heißt große und kleine Buchstaben, Ziffern und mindestens ein Sonderzeichen bei einer Länge von wenigstens 10 Zeichen enthalten. Wer vermutet, dass sein Passwort anderen Personen bekannt geworden ist, ändert dieses.

3. Eingriffe in die Hard- und Softwareinstallation

Veränderungen der Installation und Konfiguration der Arbeitsstationen und des Netzwerks sowie Manipulationen an der Hardware- und Softwareausstattung sind grundsätzlich untersagt. Dies gilt nicht, wenn Veränderungen auf Anordnung der Systembetreuung durchgeführt werden oder wenn temporäre Veränderungen im Rahmen des Unterrichts explizit vorgesehen sind. Die SuS dürfen sich nur mit einem Gerät im WLAN der Schule anmelden. Dazu bedarf es zwingend der

Unterzeichnung der Nutzungsvereinbarung der Schule.
Die Schule übernimmt keine Haftung für Fremdgeräte und deren Datensicherheit, die Verantwortung dafür liegt ausschließlich bei den Nutzerinnen und Nutzer und kann nicht auf andere übertragen werden. Schad- und Virenschutzsoftware auf dem Fremdgerät ist stets aktuell zu halten und Sicherheitsupdates werden von den Nutzerinnen und Nutzern entsprechend installiert. Andere Peripheriegeräte wie externe Datenspeicher dürfen nur mit Zustimmung der Systembetreuung an Computern der Schule genutzt werden. Diese sollten eine Namensdatei enthalten und vor jedem Einsatz in der Schule auf einen Befall durch Schadsoftware geprüft werden. Insbesondere dürfen keine Dateien oder Skripte auf dem externen Datenspeicher ausgeführt werden. Schuleigene Geräte dürfen grundsätzlich nicht an Dritte weitergegeben und nur für unterrichtliche Zwecke genutzt werden.
Im Allgemeinen ist ein unnötiges Datenaufkommen durch Laden und Versenden großer Dateien (etwa Filme) aus dem Internet zu vermeiden. Sollte ein Nutzer unberechtigt größere Datenmengen in seinem Arbeitsbereich ablegen, ist die Schule berechtigt, diese Daten zu löschen. Die Beeinträchtigung des Netzbetriebes durch ungezielte und übermäßige Verbreitung von Daten bzw. durch unsachgemäßen Einsatz von Hard- und Software, jede Art des Mithörens oder Protokollierens von fremdem Datenübertragungen, des unberechtigten Zugriffs auf fremde Datenbestände oder der unberechtigte Zugang zu fremden Rechnern oder die Manipulationen von Informationen ist untersagt.

4. Verbotene Nutzungen

Die gesetzlichen Bestimmungen – insbesondere des Datenschutzes, des Strafrechts, des Urheberrechts und des Jugendschutzrechts – sind zu beachten. Es ist verboten, pornographische, gewaltverherrlichende oder rassistische Inhalte aufzurufen oder zu versenden. Werden solche Inhalte versehentlich aufgerufen, ist die Anwendung zu schließen und der Aufsichtsperson Mitteilung zu machen. Verboten ist beispielsweise auch die Nutzung von Online-Tauschbörsen. Aus Datenschutzgründen dürfen keine Schuldaten auf externe Server hochgeladen werden.

5. Protokollierung des Datenverkehrs

Die Schule ist in Wahrnehmung ihrer Aufsichtspflicht berechtigt, den Datenverkehr zu speichern und zu kontrollieren. Dazu arbeitet sie auch mit dem IT-Dienstleister der Schule zusammen. Diese Daten werden in der Regel nach 90 Tagen gelöscht. Dies gilt nicht, wenn Tatsachen den Verdacht eines schwerwiegenden Missbrauches der schulischen Computer oder des Wlans begründen. In diesem Fall werden die gespeicherten Protokolldaten ausgewertet und die personenbezogenen Daten werden bis zum Abschluss der Prüfungen und Nachforschungen gespeichert. Die Schulleitung

oder von ihr beauftragte Personen werden von ihren Einsichtsrechten nur stichprobenartig oder in Fällen des Verdachts von Missbrauch Gebrauch machen. Dabei gilt ein Vier-Augen-Prinzip. Die Auswertung der Protokolldaten wird schriftlich dokumentiert. Eine Auswertung zu statistischen Zwecken erfolgt nicht.

6. Nutzung von Informationen aus dem Internet

Die Nutzung der IT-Systeme und des Internets ist nur im Unterricht als Lehr- und Lernmittel und außerhalb des Unterrichts zu unterrichtlichen Zwecken zulässig. Dadurch ergeben sich einerseits vielfältige Möglichkeiten, pädagogisch wertvolle Informationen abzurufen, zum anderen besteht jedoch die Gefahr, dass Schülerinnen und Schüler Zugriff auf Inhalte erlangen, die ihnen nicht zur Verfügung stehen sollten. Die Schule bemüht sich durch Filterung und Firewallregeln dies zu verhindern, kann aber den Schutz nicht garantieren. Die Nutzung der IT-Systeme und des Internets zu privaten Zwecken, insbesondere für soziale Netzwerke und Messengerdienste, ist

nicht gestattet. Als schulisch ist ein elektronischer Informationsaustausch anzusehen, der unter Berücksichtigung seines Inhalts und des Adressatenkreises mit der schulischen Arbeit im Zusammenhang steht. Das Herunterladen von Anwendungen ist nur mit Einwilligung der Schule
zulässig. Die Schule ist nicht für den Inhalt der über ihren Zugang abrufbaren Angebote Dritter im Internet verantwortlich. Im Namen der Schule dürfen weder Vertragsverhältnisse eingegangen noch kostenpflichtige Dienste im Internet benutzt werden. Beim Herunterladen wie bei der Weiterverarbeitung von Daten aus dem Internet sind insbesondere Urheber- oder Nutzungsrechte zu beachten.

7. Verbreiten von Informationen im Internet

Die Schülerinnen und Schüler nutzen das Internet verantwortungsbewusst. Sie sollen nichts über sich veröffentlichen, was sie nicht auch einem Fremden auf der Straße beziehungsweise ihrem Gegenüber ins Gesicht sagen würden. Werden Informationen im bzw. über das Internet verbreitet, geschieht das unter Beachtung der allgemein anerkannten Umgangsformen. Die Veröffentlichung von Internetseiten der Schule oder im Namen der Schule bedarf ausdrücklich der Genehmigung durch die Schulleitung. Für fremde Inhalte sind insbesondere der Datenschutz und das Urheberrecht zu beachten. So dürfen beispielsweise digitalisierte Texte, Bilder und andere Materialien nur mit Zustimmung des Rechteinhabers auf Internetseiten verwendet oder über das Internet verbreitet werden. Werke von anderen Personen müssen als solche gekennzeichnet werden. Das Recht am eigenen Bild und das allgemeine Persönlichkeitsrecht sind zu beachten. Foto-, Audio- und Videoaufnahmen dürfen nur mit Erlaubnis der Lehrkraft gemacht werden. Die Aufnahmen dürfen nur innerhalb des Unterrichts auf den privaten Geräten genutzt werden. Die Aufnahmen sind nach Abschluss des Arbeitsauftrags zu löschen. Aufnahmen, die im Unterricht gemacht wurden, dürfen grundsätzlich nicht Dritten gezeigt, an Dritte weitergegeben oder im Internet veröffentlicht werden. Daten von Lehrkräften, Schülerinnen und Schülern sowie Erziehungsberechtigten dürfen im Internet nur veröffentlicht werden, wenn die Betroffenen schriftlich eingewilligt haben. Alle Inhalte, die Lehrkräfte im Rahmen des Unterrichts in der Schule oder für das Lernen zu Hause zur Verfügung stellen, unterliegen dem Urheberrecht, sind ausschließlich für den persönlichen Gebrauch und dürfen nicht an Dritte weitergegeben werden. Bei allen anderen Angehörigen der Schulgemeinschaft gilt: Bei Minderjährigen bis zur Vollendung des 14. Lebensjahres ist dabei die Einwilligung der Erziehungsberechtigten, bei Minderjährigen ab der Vollendung des 14. Lebensjahres deren Einwilligung und die Einwilligung der Erziehungs-berechtigten erforderlich. Die Einwilligung kann ohne Angabe von Gründen widerrufen werden. In diesem Fall sind die Daten zu löschen. Persönliche Fotos und Daten, die Rückschlüsse auf eine bestimmte Person zulassen,

werden nicht ohne deren Einwilligung weitergegeben. Auch bei der Weiterverarbeitung sind Urheber- und Nutzungsrechte zu beachten. Die Schülerinnen und Schüler werden auf die Gefahren hingewiesen, die mit der Verbreitung persönlicher Daten im Internet einhergehen. Weiterhin wird auf einen verantwortungsbewussten Umgang der Schülerinnen und Schüler mit persönlichen Daten hingewirkt.

8. Verantwortlichkeit der Nutzerinnen und Nutzer

Schülerinnen und Schüler halten bei der Nutzung der IT-Systeme und des Internets gesetzliche Vorschriften sowie die Regelungen der Nutzungsordnung ein. Nutzer, die unbefugt Software oder Daten von den Arbeitsstationen, den iPads oder aus dem Netz kopieren oder verbotene Inhalte nutzen, können strafrechtlich sowie zivilrechtlich belangt werden. Zuwiderhandlungen gegen diese Nutzungsordnung können neben dem Entzug der Nutzungsberechtigung auch schulordnungsrechtliche Maßnahmen zur Folge haben.

C. Schlussvorschriften

Diese Nutzungsordnung ist Bestandteil der jeweils gültigen Hausordnung und tritt mit sofortiger Wirkung in Kraft. Einmal zu jedem Schuljahresbeginn findet eine Nutzerbelehrung statt. Es besteht kein Rechtsanspruch auf die Nutzung der schulischen IT-Infrastruktur für den Unterricht. Insbesondere bei Verstößen gegen die Nutzungsordnung besteht die Möglichkeit eines teilweisen oder dauerhaften Ausschlusses von der Nutzung. Die Nutzung darf Dritten über schülereigene oder schuleigene Geräte nicht gestattet werden, da jeder für alle Handlungen einsteht, die mit seinen Zugangsdaten vorgenommen wurden.

Nutzungsordnung für Schülerinnen und Schüler
für die Verwendung der MNSpro Cloud (inkl. Microsoft Office 365) an der Bischöflichen St. Angela-Schule Düren

1. Worum handelt es sich?

Die Bischöfliche St. Angela-Schule Düren stellt für das gemeinsame Arbeiten und Lernen im Unterricht und zu Hause die MNSpro Cloud inklusive Microsoft Office 365 (im Folgenden „Office 365“) zur Verfügung. Der Zugang zu Office 365 wird auch außerhalb des Unterrichts zur rein schulischen Nutzung zur Verfügung gestellt. Diese Nutzungsordnung informiert und steckt den Rahmen für eine verantwortungsvolle Nutzung ab.

Mit den Diensten, Programmen und Apps können Sie mit Lehrkräften und anderen Schülerinnen und Schülern im Unterricht zusammenarbeiten. Die Programme, Dienste und Apps können Sie auch zu Hause zum Lernen und Arbeiten für die Schule verwenden.

2. Geltungsbereich

Diese Nutzungsordnung gilt für die rein schulische Benutzung von Office 365 durch Schülerinnen und Schüler der Bischöflichen St. Angela-Schule Düren. Eine private Nutzung von Office 365 muss unterbleiben, um die im System vorhandene Pseudonymisierung nicht zu unterlaufen.

3. Wie lange darf ich Office 365 verwenden?

Sie dürfen Office 365 so lange verwenden, wie Sie an der Schule angemeldet sind. Wenn Sie die Schule verlassen, wird Ihr Benutzerkonto regelmäßig nach spätestens 12 Wochen gelöscht. Dann können Sie die Dienste, Programme und Apps nicht mehr nutzen. Das rechtzeitige Sichern Ihrer Dateien und Daten liegt in Ihrer eigenen Verantwortung.

4. An welche Regeln muss ich mich halten?

Halten Sie sich an folgende Regeln:

Sie sind verpflichtet sich bei der Nutzung von Office 365 an das geltende Recht zu halten. Nehmen Sie keine unrechtmäßigen Handlungen vor.

Verletzen Sie keine Rechte anderer und halten Sie sich an die Regeln des Urheberrechts! Fremde Inhalte (Texte, Fotos, Videos, Lieder, Audio und andere Materialien) dürfen Sie nicht ohne Genehmigung der Urheber in Office 365 speichern. Dazu gehören auch eingescannte oder abfotografierte Texte und Bilder.

Unterlassen Sie es, unangemessene Inhalte oder anderes Material (das z. B. Nacktdarstellungen, Brutalität, Pornografie, anstößige Sprache, Gewaltdarstellungen oder kriminelle Handlungen zum Inhalt hat) zu veröffentlichen oder über die Dienste zu teilen.

Die Verbreitung und das Versenden von belästigenden, beleidigenden oder bedrohenden Inhalten sind verboten.

Unterlassen Sie Handlungen, durch die andere ausgenutzt werden, ihnen Schaden zugefügt oder angedroht wird.

Durch die E-Mail-Funktion dürfen Sie keine Massen-Nachrichten (Spam) und/oder andere Formen unzulässiger Werbung versenden.
Unterlassen Sie Handlungen, die betrügerisch, falsch oder irreführend sind (z. B. sich als jemand anderes ausgeben oder versuchen die Dienste zu manipulieren).
Unterlassen Sie es, wissentlich Beschränkungen des Zugriffs auf bzw. der Verfügbarkeit der Programme und Apps zu umgehen.
Unterlassen Sie Handlungen, die Ihnen oder anderen Schaden zufügen (z. B. das Übertragen von Viren, das Belästigen anderer, das Posten terroristischer Inhalte, Hassreden oder Aufrufe zur Gewalt gegen andere).
Unterlassen Sie Handlungen, die die Privatsphäre von anderen verletzen.
Helfen Sie niemandem bei einem Verstoß gegen diese Regeln.

5. Nutzungsbedingungen von Microsoft Office 365

Es gelten außerdem die Nutzungsbedingungen des Microsoft-Servicevertrags: https://www.microsoft.com/de-de/servicesagreement/ Es wird vor allem auf den diesbezüglichen Verhaltenskodex hingewiesen.

6. Wie ist es mit Schutz und Sicherheit meiner (personenbezogener) Daten?

Die Bischöfliche St. Angela-Schule Düren hat die notwendigen Auftragsverarbeitungsverträge gemäß KDG abgeschlossen, welche gewährleisten, dass personenbezogene Daten von Benutzern nur entsprechend der Vertragsbestimmungen verarbeitet werden. Durch eine Minimierung von personenbezogenen Daten bei der Nutzung von Office 365 auf das erforderliche Maß, soll das Recht auf informationelle Selbstbestimmung unserer Schülerinnen und Schüler sowie des pädagogischen Personals bestmöglich geschützt werden. Dies 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.

6.1 Pseudonymisierung

Die Nutzung von Office 365 erfolgt für Schülerinnen und Schüler durch pseudonymisierte E-Mail-Adressen und pseudonymisierte Nutzeraccounts. Dies ist eine zwingend umzusetzende Maßnahme, um die personenbezogenen Daten von Schülerinnen und Schülern zu schützen.

Die Pseudonymisierung darf weder durch Schülerinnen und Schüler noch durch Lehrkräfte aufgelöst werden und ist zwingend einzuhalten. Es ist nicht gestattet, innerhalb der Office 365 Umgebung Klarnamen zu verwenden (z. B. in Chatnachrichten oder in Dokumenten).

6.2 Auswahl und Klassifizierung der Daten

Die Datenbearbeitung hat sich nach den schulischen Aufgaben und Zwecken zu richten. Nicht alles, was möglich ist, ist erlaubt. Es ist sicherzustellen, dass nur die Daten bearbeitet werden,

die für die jeweilige Aufgabenerfüllung und den jeweiligen Zweck notwendig sind. Die Daten sind den folgenden Schutzbedarfskategorien zuzuordnen:

- **Gering**: Personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen nicht beeinträchtigt werden kann. Beispiel: Arbeitsblätter mit Pseudonym
- **Normal**: Personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann. Beispiel: Arbeitsergebnisse mit Pseudonym.
- **Hoch**: Personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann. Hierunter fallen auch personenbezogene Daten nach § 203 StGB (Verletzung von Privatgeheimnissen) und besonders schutzwürdige personenbezogene Daten sowie Personalaktendaten. Beispiel: vertrauliche Kommunikation mit Vertrauenslehrerinnen und Vertrauenslehrern.
- **Sehr hoch:** Personenbezogene Daten, bei deren Verarbeitung eine Gefahr für Leib und Leben oder die persönliche Freiheit des Betroffenen gegeben ist. Beispiel: Auskunftssperre, Zeugenschutzprogramm. Hierbei wird davon ausgegangen, dass diese Daten im schulischen Kontext und der geplanten Datenverarbeitung nicht verarbeitet werden.

Mit Office 365 dürfen ausschließlich Daten der Kategorien „gering“ und „normal“ bearbeitet werden. Für Datenverarbeitungen der Kategorien „hoch“ und „sehr hoch“ gibt es keine Freigabe durch die Vorgaben des Datenschutzes und der IT-Sicherheit; auch die erforderlichen Schutzmaßnahmen sind auf diese Kategorien nicht ausgelegt.

Die Verarbeitung von besonderen Kategorien personenbezogener Daten ist unzulässig. Dazu gehören z. B. Gesundheitsdaten, politische Meinungen, Daten zur sexuellen Orientierung und Daten, aus denen die religiösen oder weltanschaulichen Überzeugungen von Personen hervorgehen. Bei Aufgabenstellungen in allen Unterrichtsfächern ist darauf zu achten, dass besondere Kategorien personenbezogener Daten in der Office 365 Umgebung nicht verarbeitet werden.

Ein Beispiel: Schülerinnen und Schüler sollen einen Aufsatz mit Ihrer persönlichen Meinung zu einem Wahlprogramm einer Partei (politische Meinungen) oder einen Aufsatz mit Ihrer persönlichen Meinung und den Gründen für und gegen Abtreibungen (weltanschauliche Überzeugungen) verfassen. Diese Aufgaben dürfen nicht in der Office 365 Umgebung erstellt, gespeichert und geteilt werden.

6.3 Umgang mit personenbezogenen Daten in Office 365

- In der Cloud (OneDrive) sollen nur unter sorgfältiger Abwägung personenbezogene Daten versendet bzw. gespeichert werden und nur, wenn es aufgrund schulischer Erfordernisse bzw. zur Aufgabenerfüllung notwendig ist. Es gelten die Prinzipien der Datenminimierung und Datensparsamkeit.
- Werden personenbezogene Daten in der Cloud gespeichert, sollen diese zum Schutz vor einem Fremdzugriff durch Passwörter (Dokumentkennwort) und/oder mit einem geeigneten Programm verschlüsselt werden (z.B. 7-Zip).

- Besonders schutzwürdige personenbezogene Daten dürfen nicht in der Office 365 Umgebung gespeichert werden.
- Eine Weiterleitung an oder eine Offenlegung gegenüber Dritten ist untersagt. Ebenso ist das Zugänglichmachen von Daten an Dritte auf andere Art und Weise untersagt.

6.4 Löschen

Die personenbezogenen Daten dürfen nur für die Dauer der Schulzugehörigkeit gespeichert werden und sind dann zu löschen. Für die Sicherung der Daten sind die jeweiligen Schülerinnen und Schüler selbst verantwortlich. Eine Sicherung hat außerhalb der Office 365 Umgebung zu erfolgen. Die Löschung der Protokolldaten erfolgt automatisiert. Diese Speicherfrist beträgt 90 Tage.

6.5 Passwörter

Für die Nutzung von Office 365 ist ein ausreichend sicheres Passwort zu wählen. Dieses ist geheim zu halten. Die Administratoren beraten hinsichtlich der Anforderungen an ein sicheres Passwort.

6.6 Protokollierung und Stichprobenartige Kontrolle

Bei der Nutzung der Dienste können Daten über die Schülerinnen und Schüler und deren Aktivitäten automatisch erfasst und gespeichert werden. Man spricht von Protokollieren respektive «Loggen». Die Protokolldaten dürfen nur bearbeitet werden, wenn dies für das Funktionieren des Systems notwendig ist. Bei Verdacht auf Missbrauch der Dienste durch die Nutzenden können Protokolldaten stichprobenweise unter Hinzuziehung der Vertrauenslehrerinnen und Vertrauenslehrer sowie des Datenschutzbeauftragten und ggf. nach vorgängiger Information der Betroffenen ausgewertet werden. Eine Leistungskontrolle diesbezüglich erfolgt nicht.

Dem betrieblichen Datenschutzbeauftragten ist es stichprobenhaft gestattet, die Einhaltung der Vorgaben dieser Nutzungsanordnung sowie weiterer Vorgaben zu kontrollieren.

6.7 Zugangsdaten

- Der Benutzerinnen und Benutzer sind 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, sind die Benutzerinnen und Benutzer verpflichtet, sofort Maßnahmen zum Schutz der eigenen Zugänge zu ergreifen. Falls noch möglich, sind Zugangspasswörter zu ändern. Ist dieses nicht möglich, ist einer der schulischen Administratoren zu informieren.
- Sollten die Benutzerinnen und Benutzer in Kenntnis fremder Zugangsdaten gelangen, so ist es untersagt, sich damit Zugang zum fremden Benutzerkonto zu verschaffen. Die

Benutzerinnen und Benutzer sind jedoch verpflichtet, den Eigentümer der Zugangsdaten oder einen schulischen Administrator zu informieren.

- Nach Ende der Unterrichtsstunde oder der Arbeitssitzung an einem schulischen Rechner bzw. schulischen Mobilgerät melden sich die Benutzerinnen und Benutzer von Office 365 ab (ausloggen).

6.8 Datenschutz und IT-Sicherheitsvorfälle

Bei Verdacht der Gefährdung der IT-Sicherheit und bei IT-Sicherheitsvorfällen ist der zuständige Administrator oder der IT-Sicherheitsbeauftragte zu verständigen. Im Umgang mit Sicherheitsvorfällen sind Ehrlichkeit und Kooperationsbereitschaft besonders wichtig. Die Meldung von Sicherheitsvorfällen wird positiv gewürdigt. Bei datenschutzrelevanten Vorfällen ist zusätzlich der betrieblich Beauftragter für den Datenschutz und die zuständige Datenschutzansprechperson der Schule zu informieren.

7. Sonderregelung zur Nutzung von Microsoft Office „Teams“

7.1 Grundlage

Mit MS Teams steht den Lehrkräften und Schülerinnen und Schülern ein leistungsfähiges Tool zur Verfügung, um Absprachen und Planungen durchzuführen und Online-Unterricht zu ermöglichen.

7.2 Nutzungsrichtlinien und Verhaltensregeln

Mit Teams sind Video- und Tonübertragungen möglich. Dies bedarf im Rahmen von Online-Abstimmungen (und Online-Unterricht) einer besonders verantwortungsvollen Nutzung. Videoübertragungen (Bild und Ton) stellen aus datenschutzrechtlicher Sicht sensible personenbezogene Daten dar. Daher beachten Sie bitte die folgenden Voraussetzungen für die Nutzung von Teams.

- Es ist zulässig, am Online-Unterricht teilzunehmen und außerhalb des Online-Unterrichtes zu schulischen Zwecken Online-Konferenzen durchzuführen.
- Bei Nutzung der Videoübertragung müssen die Personen im Kameraerfassungsbereich damit einverstanden sein. Diese Zustimmung erfolgt durch konkludentes Handeln (Aktivierung der Kameras am jeweiligen Gerät). Die Teilnehmerinnen und Teilnehmer werden zu Beginn der Besprechung hierüber aufgeklärt. Bei Video-Konferenzen bzw. Video-Unterricht ist mehr Sorgfalt bei der Bestimmung des sichtbaren Umfeldes geboten. Sie sollten daher nur bei entsprechender Erforderlichkeit durchgeführt werden und unter Verwendung des sogenannten Weichzeichners (der Hintergrund wird verschwommen dargestellt).
- Aufzeichnungen (Mitschnitte) von Konferenzen (unabhängig davon, ob eine Bildübertragung stattfindet) sind systemseitig deaktiviert und aus Teams heraus nicht möglich. Bei einer Aufzeichnung bedarf es der Zustimmung aller Beteiligten.
- Die Aufzeichnung (Erstellung von Mitschnitten) von Konferenzen durch andere mobile Endgeräte (z. B. Smartphone) ist nicht gestattet.

- Die Freigabe von Teams ist auf Inhalte mit normalem Schutzbedarf (s.o.) beschränkt. Geteilte Dokumente in Teams-Chats mit personenbezogenen Daten sind mit einem Kennwort vor unberechtigtem Zugriff zu schützen.
- Eine Weiterleitung oder Offenlegung von Inhalten der Sitzungen an Dritte oder das Zugänglichmachen von Teams-Sitzungen für Dritte ist untersagt und systemseitig unterbunden.
- Desktop-Sharing (d.h. das Übertragen des gesamten Desktop-Inhalts oder bestimmter Desktop-Fenster) ist erlaubt. Es ist aber stets zu prüfen, ob dies im Einzelfall erforderlich ist (wovon i.d.R. bei Online-Unterricht ausgegangen werden kann) oder das Teilen von Dokumenten nicht ausreichend ist. Bevor der Desktop für andere freigegeben wird, ist sorgfältig zu prüfen, ob ggf. Programme bzw. Fenster mit sensiblen Inhalten geöffnet sind (z.B. persönliches E-Mail-Postfach). Diese sind vorher zu schließen. Die Icons auf dem Desktop sind darauf zu prüfen, ob Benennungen enthalten sind, die vor den Konferenzteilnehmern zu verbergen sind.
- Die Schülerinnen und Schüler sind verpflichtet die gesetzlichen Regelungen des Straf- und Jugendschutzes sowie das Urhebergesetz zu beachten. Die Lehrkräfte werden ihre Schülerinnen und Schüler explizit auf die Folgen von Fehlverhalten hinzuweisen.
- Die Sicherung der in Teams gespeicherten Daten gegen Verlust obliegt der Verantwortung den Schülerinnen und Schülern.
- Die Administration ist berechtigt, im Falle von konkreten Verdachtsmomenten von missbräuchlicher oder strafrechtlich relevanter Nutzung des Dienstes die jeweiligen Inhalte (Chats, Dateien etc.) zur Kenntnis zu nehmen. Die betroffenen Nutzer werden hierüber unverzüglich informiert.
- Im Fall von Verstößen gegen die Nutzungsordnung kann das Konto gesperrt werden. Damit ist die Nutzung von Office365 und Teams nicht mehr möglich

Aufbewahrung und Löschung

- Nicht (mehr) benötigte Teams und deren Daten sind umgehend durch die Administratoren zu löschen. Die Sicherung der Daten liegt in der Verantwortung der Teams-Mitglieder.

8. Die Team-Mitglieder sind über die jeweiligen für das konkrete Team geltenden Löschungen zu informieren. Eingriffe in die Hard- und Softwareinstallation

Veränderungen der Installation und Konfiguration der schulischen Arbeitsstationen/des Netzwerkes etc. sowie Manipulation an der schulischen Hardwareausstattung sind grundsätzlich untersagt.

Veränderungen der Installation und Konfiguration von Office 365 sind untersagt.

Die festgelegten Regeln habe ich zur Kenntnis genommen und halte diese ein. Sollte ich gegen die Nutzungsregeln verstoßen, verliere ich meine Nutzungsberechtigung und muss mit

schulrechtlichen Maßnahmen rechnen. Bei Verstoß gegen gesetzliche Bestimmungen sind weitere zivil- oder strafrechtliche Folgen nicht auszuschließen.

Regelungen für den Umgang mit Smartphones

Sehr geehrte Eltern, liebe Schülerinnen und Schüler, liebe Kolleginnen und Kollegen,

für den Umgang mit Smartphones an unserer Schule sind diese Regelungen von der Schulkonferenz in ihrer Sitzung vom 22. September 2022 genehmigt worden und sind ab sofort in modifizierter Form verbindlich für die gesamte Schule **und gelten mit dem Betreten des Schulgeländes.**

- Zu unterrichtlichen Zwecken ist die Nutzung von Smartphones und allen Diensten erlaubt.
- Allen Schülerinnen und Schülern ist während und außerhalb des Unterrichts immer und überall in der Schule Gaming und Streaming verboten.
- In der **Mittagspause** ist die Nutzung von Smartphones allen Schülerinnen und Schülern prinzipiell erlaubt, auch für social media und messenger Dienste.
- In der **Mensa** ist die Nutzung von Smartphones den Schülerinnen und Schülern aller Jahrgangsstufen immer und zu allen Zeiten verboten.
- Der **Oberstufe** ist zu jedem Zeitpunkt die Nutzung von Smartphones erlaubt: Während der Unterrichtszeit in Absprache mit der Lehrkraft, außerhalb der Unterrichtszeiten bewegen sich die Schülerinnen und Schüler eigenverantwortlich im Netz. Während der Pausenzeiten ist die Nutzung nur im Kursraum und im Oberstufenbereich vor Raum K3 gestattet. Das Nutzen von Gaming und Streaming Diensten ist immer untersagt.
- Telefonieren ist allen Schülerinnen und Schülern nur in Absprache mit einer Lehrkraft erlaubt.
- Es müssen immer alle Klingeltöne auf „stumm“ geschaltet sein.

Sanktionen

1. Stufe: Abnahme und Lagerung des Geräts im Sekretariat (Abholung frühestens 13.05 Uhr)
2. Stufe: Eltern müssen das Endgerät abholen. Öffnungszeiten des Sekretariats beachten.
3. Stufe: Das Gerät darf eine Woche lang nicht mit in die Schule gebracht werden

Informationen zur Datenverarbeitung im Rahmen der Nutzung von elternfinanzierten iPads

An der Bischöflichen St. Angela-Schule Düren nutzen Schülerinnen und Schüler sowie Lehrerinnen und Lehrer iPads. Damit das möglich ist, werden auch personenbezogene Daten der Benutzer von der Schule und von Jamf School, der Plattform, mit welcher Nutzer und iPads verwaltet werden, verarbeitet. Hiermit möchten wir Ihnen/ dir gemäß den Anforderungen aus §§ 15,16 KDG alle wichtigen Informationen zur Datenverarbeitung bereitstellen. Diese Informationen beziehen sich im Hinblick auf Apple nur auf iPads, iOS und Apple eigene Apps. Apps anderer Anbieter sind hier nicht berücksichtigt. Diese Informationen zur Datenverarbeitung im Zusammenhang mit der Nutzung von iPads gelten für alle schulischen Nutzer von iPads (Schülerinnen und Schüler, Lehrerinnen und Lehrer sowie schulisches Personal).

Wer ist für die Verarbeitung meiner Daten verantwortlich und an wen kann ich mich zum Thema Datenschutz wenden?

Verwaltungsdienstleiter und Aufsichtsstelle ist die Schulabteilung des Bischöflichen Generalvikariates Aachen (BGV). Der Schulträger und die Schule unterliegen den kirchlichen Datenschutzbestimmungen, insbesondere dem Gesetz über den kirchlichen Datenschutz (KDG), das mit der europäischen Datenschutz-Grundverordnung (EU-DSGVO) gemäß Artikel 91 DSGVO in Einklang gebracht wurde.

Schulträger:

Bistum Aachen
Körperschaft des öffentlichen Rechts

Vertreten durch: Dr. Andreas Frick, Generalvikar

Klosterplatz 7, 52062 Aachen
Tel: 0241 452-0
E-Mail: kommunikation@bistum-aachen.de

Schule:

Bischöfliche St. Angela- Schule
Bismarckstraße 24, 52351 Düren

Schulleiter: Herr OStD i.K. Olaf Windeln

Telefon: (02421) 1 60 41
Telefax: (02421) 2 07 96 42
E-Mail: sekretariat@angela-dueren.de

Betrieblicher Datenschutzbeauftragter:

Herr Holger Brinkmeyer
Datenschutz Nord GmbH
Konsul-Smidt-Str. 88, 28217 Bremen

Telefon: (0421) 6966320
E-Mail: hbrinkmeyer@datenschutz-nord.de / datenschutz@bistum-aachen.de

Woher kommen meine Daten und welche Daten werden verarbeitet?

Beim Kauf der iPads über den Webshop der Schule, welcher durch die ACS Group angeboten wird, werden folgende Daten an ACS Group weitergeleitet: Name, Vorname, Klassenzugehörigkeit.

ACS Group verifiziert den Kauf und leitet die iPads an den Dienstleister WMS (WMS Webmad Systemhaus GmbH) weiter. Dort erfolgt die Einrichtung von Rechten und Rollen der Geräte entsprechend Ihrer Funktion (Schüler / Lehrkraft) und der Zugehörigkeit zu Klassen und Gruppen und die Berechtigung zur Nutzung des WLANs. WMS richtet dazu die Applikation

Jamf school als Mobil Device Management (MDM) ein und verbindet Ihr iPad mit der Schule, sodass von dort die Administration erfolgen kann. Hierbei werden die Gerätenamen und die Seriennummer einer entsprechenden Gruppe (Klassenzugehörigkeit) zugeordnet.

Weitere Daten entstehen bei der Nutzung der iPads und des MDM im Unterricht und bei der Vor- und Nachbereitung des Unterrichts:

- Benutzerdaten (z.B. Anmeldenamen, Kennwort, Gruppenzugehörigkeit, Gerätezuweisungen)
- Installierte Applikationen (keine Inhaltsdaten innerhalb der Applikationen),
- Benutzerverwaltung, Gerätemanagement, Benutzergruppen
- Technische Nutzungsdaten und Log-Files: System-Logs zur Gewährleistung des ordnungsgemäßen Betriebs und der Verfügbarkeit; Metadaten von Dokumenten und Dateien; Zeitpunkt, Sender, Empfänger

Wofür werden meine Daten verwendet (Zweck der Verarbeitung) und auf welcher Basis (Rechtsgrundlage) passiert dies?

- Vorbereitung und Durchführung von Unterricht
- (technische) Verwaltung von Rechten und Rollen der Benutzer entsprechend der Funktion (Schülerinnen und Schüler/ Lehrerinnen und Lehrer) und der Zugehörigkeit zu Klassen und Gruppen (z. B., um Inhalte im Internet zu sperren)
- Berechtigung zur Nutzung des WLANs
- Zuordnung von iPads, Apps, digitalen Büchern, Materialien
- Technische Bereitstellung von Daten für die Verwaltung und Nutzung von iPads und damit zusammenhängenden Diensten Jamf School
- Einbindung in das schulische Netzwerk zur Bereitstellung von Unterrichtsinhalten
- Sicherheit und Funktionalität dieser Dienste

Die Verarbeitung erfolgt auf der Grundlage des Schulvertrages, den die Erziehungsberechtigen mit der Schule eingehen (§ 6 Abs. 1 lit. c) KDG) und durch rechtliche Verpflichtungen, die von der Bischöflichen St. Angela-Schule Düren zu erfüllen, z.B. gemäß § 120 Abs. 5 Schulgesetz NRW (§ 6 Abs. 1 lit. d) KDG). Außerdem ist die Verarbeitung von Daten zur Sicherstellung eines ordnungsgemäßen Betriebs der digitalen Unterrichtseinheiten erforderlich.

Werden meine Daten weitergegeben und wer hat Zugriff auf meine Daten?

Die Nutzung von iPads und Apps ist nur möglich, wenn man dafür von Apple bereitgestellte Dienste nutzt. Dieses sind Dienste zur Verwaltung von iPads, Nutzern, Apps und Inhalten. Der Zugriff auf diese Dienste erfolgt über eine von einem Anbieter zur Verfügung gestellte Verwaltungsoberfläche, ein Mobile Device Management (MDM). Der Anbieter ist ein sogenannter Auftragsverarbeiter – er verarbeitet alle Daten nach Weisung durch den Schulträger:

Vom Schulträger beauftragter Dienstleister:

WMS Webmad Systemhaus GmbH
Kieselstraße 6-8, 41472 Neuss
WMS unterstützt die Schule bei der Installation des Mobile Device Managements sowie im Support der schulischen Administratoren.

ACS GROUP GmbH Otto-Hahn-Str. 38a, 85521 Ottobrunn

ACS Group betreibt den schuleigenen Webshop über den die IPads erworben werden können.

Innerhalb der Schule wird der Zugriff auf die Daten im Zusammenhang mit der Nutzung von iPads durch das Rechte- und Rollenkonzept geregelt.

- Lehrerinnen und Lehrer: Eigene Daten und Daten von Lernenden und Lehrenden werden entsprechend ihrer Funktion und Freigaben durch die Personen selbst an ausgewählte Personen innerhalb der Schule weitergeben.
- Schülerinnen und Schüler: Eigene Daten und Daten von Mitschülerinnen und Mitschülern werden entsprechend nach Freigaben von Lehrerinnen und Lehrer bzw. Schülerinnen und Schülern an ausgewählte Personen innerhalb der Schule weitergegeben.

Personen außerhalb der Schule erhalten nur Zugriff auf Daten, wenn ein Gesetz es ihnen gestattet. Darüber hinaus bestehen folgende Möglichkeiten, dass Personen von außerhalb Daten einsehen:

- Eltern, bei Freigabe durch Schülerinnen und Schüler,
- Eltern und (ehemalige) Schülerinnen und Schüler (Auskunftsrecht nach § 17 KDG)
- Ermittlungsbehörden im Fall einer Straftat

In solchen Fällen erfolgt ein Zugriff nur auf die eigenen, die betroffene Person betreffende Daten, und regelhaft kein Zugriff auf die Daten Dritter.

Werden meine Daten in ein Drittland oder an eine internationale Organisation übermittelt?

Mit dem Kauf des iPads werden diese durch ACS GROUP als zertifizierter Partner von Apple registriert. Hierbei findet ein Abgleich dahingehend statt, dass das gekaufte Gerät legal erworben wurde. Die Seriennummern der iPads sind jedoch auf das Bistum registriert, sodass hier keine Übermittlung personenbezogener Daten stattfindet.

Sofern Sie bereits über ein IPad verfügen, welches Sie für die schulische Nutzung zur Verfügung stellen wollen, entfällt die Registrierung über ACS Group, da die Registrierung bereits beim Kauf Ihres IPads erfolgt ist. Das IPad wird dann direkt durch WMS eingerichtet.

Bei der Installation des Mobile Device Management Jamf school durch WMS werden diese Seriennummern mit Jamf verbunden, sodass dem Mobile Device Management bekannt ist, welche Seriennummer zur Bischöflichen St. Angela-Schule Düren gehört. Ebenfalls wird in der

Jamf-Administration das jeweilige Gerät einer Schülerin bzw. einem Schüler zugewiesen. Dieser Vorgang kann als Heirat bezeichnet werden.

Es ist möglich, dass im Rahmen der dargestellten Datenverarbeitungen personenbezogene Daten an Anbieter aus den USA übermittelt werden. Eine Verarbeitung der personenbezogenen Daten findet damit auch in einem Drittland statt. Nach einem Urteil des Europäischen Gerichtshofs (C-311/18 vom 16. Juli 2020) werden die USA als ein Land mit einem nach EU-Standards unzureichendem Datenschutzniveau eingeschätzt. Die Übermittlungsbefugnis ergibt sich aus dem Vertrag, welchen Sie mit der Bischöfliche St. Angela-Schule Düren geschlossen haben (vgl. § 41 Abs. 2 KDG).

Mögliche Risiken, die sich im Zusammenhang mit den vorgenannten Datenübermittlung aktuell nicht vollständig ausschließen lassen, sind insbesondere:

- Ihre personenbezogenen Daten könnten möglicherweise über den eigentlichen Zweck der Auftragserfüllung hinaus durch die Anbieter an andere Dritte weitergegeben werden, die z. B. Ihre Daten zu Werbezwecken verwenden.
- Sie können Ihre Auskunftsrechte gegenüber den Anbietern möglicherweise nicht nachhaltig geltend machen bzw. durchsetzen.
- Es besteht möglicherweise eine höhere Wahrscheinlichkeit, dass es zu einer nicht korrekten Datenverarbeitung kommen kann, da die technischen und organisatorischen Maßnahmen der Anbieter zum Schutze personenbezogener Daten quantitativ und qualitativ nicht vollumfänglich den Anforderungen des KDG entsprechen.
- Behörden und Geheimdienste der USA könnten im Rahmen ihrer Befugnisse Einsicht in die personenbezogenen Daten erhalten.

Die Bischöfliche St. Angela-Schule Düren hat daher mit den Anbietern einen Vertrag auf Grundlage der Standardvertragsklauseln der EU-Kommission abgeschlossen, der den Anforderungen von Art. 28 DSGVO (analog dem KDG) entspricht. Darüber hinaus hat sich der Anbieter freiwillig dem EU-U.S. Data Privacy Framework unterworfen, was eine zusätzliche Sicherheit bezüglich der Datenverarbeitung darstellt.

Findet bei der Datenverarbeitung eine automatisierte Entscheidungsfindung statt?

Nein, es findet keine automatisierte Entscheidungsfindung statt. Ebenfalls findet keine automatisierte Profilbildung statt.

Wie lange werden meine Daten gespeichert?

Die Benutzerdaten der schulischen Nutzer werden so lange gespeichert wie diese

- ein iPad als Schülerinnen und Schüler nutzen, oder
- an der Schule sind, oder

der Verarbeitung ihrer Daten nicht widersprochen haben. Nach Beendigung der iPad Nutzung, Verlassen der Schule bzw. Ende des Dienstes an Schule oder Widerspruch wird die Löschung wie folgt umgesetzt:

- Daten des Benutzers unverzüglich, spätestens innerhalb von 90 Tagen auf Jamf School

Hat die Schule Einsicht in Daten, die ich außerhalb der Schule erstelle?

Die Schule hat keine Einsicht in personenbezogene Daten, die auf dem Gerät erstellt bzw. gespeichert werden. Das Mobile Device Management verfolgt lediglich den Zweck, während der Unterrichtszeiten eine Nutzung bestimmter Applikationen (z. B. YouTube) zu unterbinden oder zuzulassen. Das Mobile Device Management ist zudem so eingerichtet, dass außerhalb der Schule eine private Nutzung nicht unterbunden wird.

Welche Rechte habe ich gegenüber der Schule und dem Schulträger?

Da personenbezogene Daten bei der iPad-Nutzung verarbeitet werden, haben die Personen, deren Daten verarbeitet werden, folgende Rechte gegenüber der Schule oder dem BGV Aachen als Verantwortlichen für die Verarbeitung der Daten:

- Recht auf Auskunft über die personenbezogenen Daten (§ 17 KDG)
- Recht auf Berichtigung oder Löschung (§§ 18ff. KDG)
- Recht auf Einschränkung der Verarbeitung (§ 20 KDG)
- Recht auf Widerspruch gegen die Verarbeitung (§ 23 KDG) sowie das
- Recht auf Datenübertragbarkeit (§ 22 KDG, soweit technisch möglich).

Datenschutzrechte können bei der zuständigen Schule geltend gemacht werden. Gegebenenfalls wird die Anfrage an das BGV Aachen weitergeleitet. Betroffene erhalten die Auskunft grundsätzlich von der Stelle, bei der Rechte geltend gemacht wurden.

Recht zur Beschwerde bei der Aufsichtsbehörde

Zudem besteht das Recht auf Beschwerde bei der Datenschutzaufsichtsbehörde:

Katholisches Datenschutzzentrum
Brackeler Hellweg 144, 44309 Dortmund

Telefon: 0231/13 89 85-0
Telefax: 0231/13 89 85-22

E-Mail: info@kdsz.de
DE-Mail: info@kdsz.de-mail.de

Ist es vorgeschrieben, dass ich meine Daten zur Verfügung stelle?

Grundsätzlich sind Sie im Rahmen der Erfüllung des Schulvertrages verpflichtet Ihre personenbezogenen Daten zur Verfügung zu stellen. Diese sind: Vorname, Nachname, Klasse. Diese Daten werden dazu genutzt, einem Geräte den Besitzer eindeutig zuzuordnen. Folgen einer Nichtbereitstellung sind, dass das iPad nicht zentral während der Schulzeit administriert werden kann, d.h. das Gerät darf nicht genutzt werden. So können z. B. Apps, digitale Bücher und weitere Materialien nicht zentral für die gesamte Klasse/Kurs bereitgestellt werden. Ein Download/Installation müsste während bzw. außerhalb der Unterrichtszeit nach Anweisung der Lehrkräfte durch den Schüler oder die Schülerin eigenständig erfolgen. Des Weiteren können bestimmte Anwendungen (z. B. Apps oder Internetseiten) aufgrund deren Inhalte nicht zentral während der Unterrichtszeit gesperrt/zugelassen werden.

Sofern Gründe bestehen, die einer Bereitstellung Ihrer Daten (Vorname, Nachname, Klasse) entgegenstehen, stimmen Sie diese bitte mit der Schulleitung ab, damit eine Lösung für die Folgen der Nichtbereitstellung geprüft werden kann.

Information zur Verarbeitung personenbezogener Daten

an der Bischöfliche St. Angela-Schule Düren

Sehr geehrte Erziehungsberechtigte,

liebe Schülerinnen und Schüler,

hiermit möchten wir Ihnen gegenüber unserer **Informationspflicht nach § 15 Gesetz über den Kirchlichen Datenschutz (KDG)** zur Verarbeitung von personenbezogenen Daten in Zusammenhang mit der Nutzung der EDV-Einrichtung, des WLAN-Netzes und des Internets nachkommen. Im Folgenden informieren wir Sie über den Zweck und die rechtliche Grundlage, auf welcher wir die personenbezogenen Daten Ihres Kindes erheben und verarbeiten, an wen wir diese Daten weitergeben, wie lange wir Ihre Daten speichern und welche Rechte Sie in Bezug auf Ihre von uns verarbeiteten personenbezogenen Daten haben. Entsprechend **§ 16 KDG** informieren wir Sie auch über personenbezogenen Daten, welche wir von anderen Stellen erhalten. Für Rückfragen stehen wir Ihnen gerne zur Verfügung.

Datenverarbeitende Stelle

Bischöfliche St. Angela-Schule Düren

Bismarckstr. 24, 52351 Düren

sekretariat@angela-dueren.de

+49 2421 16041

betrieblicher Datenschutzbeauftragter

Holger Brinkmeyer

Konsul-Smidt-Str. 88, 28217 Bremen

hbrinkmeyer@datenschutz-nord.de /

datenschutz@bistum-aachen.de

+49 421 6966320

Verantwortlicher

Bischöfliches Generalvikariat Aachen

Abteilung Erziehung und Schule

Klosterplatz 7

52062 Aachen

Rechtliche Grundlagen der Datenverarbeitung

Die Verarbeitung von personenbezogenen Daten durch die Schule erfolgt gemäß § 6 KDG auf der Grundlage der Anordnung über den Kirchlichen Datenschutz für die Verarbeitung personenbezogener Daten in den katholischen Schulen in freier Trägerschaft im Bistum Aachen (KDO-Schulen), den Anlagen zur KDO-Schulen, des Schulgesetzes NRW (SchulG) und der Verordnung zur Datenverarbeitung I (VO-DV I). Rechtliche Grundlage für die Verarbeitung ist

- § 5 KDO-Schulen, § 120 Abs. 1 S. 1, Abs. 5 SchulG in Verbindung mit § 3 SchulG.
- Des Weiteren erfolgt die Datenverarbeitung gemäß § 6 Abs. 1 lit. c KDG aufgrund des Schulvertrags, den Sie mit uns schließen sowie der entsprechenden Nutzungsordnung.

- Zwecke der Datenverarbeitung
- Unterrichtsdurchführung
- Einsatz und Bereitstellung der EDV-Einrichtung und Nutzung des Internets als Lehr- und Lernmittel
- Umsetzung des Medienkonzeptes der Schule
- Protokollierung von Daten zum Schutz der EDV-Einrichtung und zur Wahrnehmung der schulischen Aufsichtspflicht

Empfänger von personenbezogenen Daten

Wir übermitteln bestimmte Daten regelmäßig oder bei Bedarf an Stellen außerhalb der Schule. Zur Bereitstellung der EDV-Einrichtung sowie des Internets übermitteln wie Ihre Daten an einen IT-Dienstleister, der diese in unseren Auftrag und nach unserer Weisung für uns verarbeiten. Mit diesem Auftragsverarbeiter haben wir einen entsprechenden Vertrag geschlossen.

Von Dritten übermittelte personenbezogene Daten

In Zusammenhang mit der Nutzung der EDV-Einrichtungen, des WLANS und des Internets erhalten wir keine personenbezogenen Daten von Schülerinnen und Schülern von Dritten.

Dauer der Speicherung

Datenarten	Aufbewahrungszeit/Löschfrist
Nutzungsdaten (Benutzername)	Nach Verlassen der Schule
Protokolldaten (Protokollierung des Datenverkehrs)	90 Tage
Protokolldaten (Protokollierung des Datenverkehrs) bei Verdacht auf schwerwiegenden Missbrauch der schulischen Computer oder des WLANS	Bis zum Abschluss der Prüfungen und Nachforschungen

Bei weiteren Daten halten wir uns an die gesetzlichen Aufbewahrungsfristen.

Ihre Pflichten als Betroffener

Es besteht kein Rechtsanspruch auf die Nutzung der schulischen EDV-Infrastruktur für den Unterricht. Insbesondere bei Verstößen gegen die Nutzungsordnung besteht die Möglichkeit eines teilweisen oder dauerhaften Ausschlusses von der Nutzung. Ohne die Bereitstellung der personenbezogenen Daten ist die Nutzung des schulischen EDV-Infrastruktur jedoch nicht möglich.

Ihre Rechte als Betroffener

Gegenüber der Schule besteht ein Recht auf **Auskunft** über Ihre personenbezogenen Daten. Ferner haben Sie grundsätzlich 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 zu.

Katholisches Datenschutzzentrum

Brackeler Hellweg 144

44309 Dortmund info@kdsz.de

0231/13 89 85-22

Unterschriftenblatt zu IT und Datenschutz

Liebe Eltern, liebe Schülerinnen und Schüler,

mit den Anmeldeunterlagen haben Sie die Informationen zum Datenschutz sowie die Nutzungsordnungen der Bischöflichen St. Angela-Schule erhalten.

Mit Ihrer Unterschrift bestätigen Sie die Kenntnisnahme dieser Regelungen und Nutzungsordnungen und erkennen diese an.

Da wir diese Kenntnisnahme und Anerkennung dokumentieren müssen, bitten wir dieses Unterschriftenblatt unterschrieben an die Schule zurückzugeben. Die Regelungen und Nutzungsordnungen bleiben zur weiteren Information und zum späteren Nachlesen in Ihrer Hand.

_____	_____	_____
Klasse	Name der Schülerin/des Schülers	Datum

Nutzungsordnung der IT-Systeme, des WLAN-Netzes und des Internets an der Bischöflichen St. Angela-Schule Düren für Schülerinnen und Schüler

Unterschrift der Schülerin / des Schülers _____

Unterschrift eines Erziehungsberechtigten _____

Nutzungsordnung für Schülerinnen und Schüler für die Verwendung der MNSpro Cloud (inkl. Microsoft Office 365) an der Bischöflichen St. Angela-Schule Düren

Mit Schreiben vom_____ wurde ich in die Nutzungsordnung für die Verwendung von Microsoft Office 365 an Schulen eingewiesen.

Unterschrift der Schülerin / des Schülers _____

Unterschrift eines Erziehungsberechtigten _____

Regelungen für den Umgang mit Smartphones

Unterschrift der Erziehungsberechtigten: _____

Unterschrift der Schülerin/des Schülers: _____

Informationen zur Datenverarbeitung im Rahmen der Nutzung von elternfinanzierten iPads

Unterschrift der Erziehungsberechtigten: _____

Unterschrift der Schülerin/des Schülers: _____

Teilnahme am Programm der elternfinanzierten iPads für Schülerinnen und Schüler im schulischen Kontext ab Klasse 7

Bischöfliche St. Angela-Schule Düren

Name, Vorname: _____

Anschrift: _____

_____

Klasse/Jgst.: _____

Gegenstand der Erklärung:

- Hiermit bestätige ich/ bestätigen wir, dass wir uns am Programm der elternfinanzierten iPads beteiligen. Wir bestätigen ferner, dass wir die Hinweise zur Datenverarbeitung zur Kenntnis genommen haben und mit den Bedingungen einverstanden sind.

Sofern Gründe vorliegen, die gegen eine Administration der iPads sprechen, wenden Sie sich an die Schulleitung oder den Schulträger.

Sofern später Gründe auftreten, werden der betreffende Account und alle zu diesem Zugang gespeicherten personenbezogenen Daten im MDM Jamf School nach dem Ablauf von 90 Tagen gelöscht, soweit keine anderweitigen gesetzlichen Pflichten der Schule dagegensprechen (z.B. Verordnung über die zur Verarbeitung zugelassenen Daten von Schülerinnen, Schülern und Eltern (VO-DV I).

Die Bestimmungen gelten bis zum Ende der Schulzugehörigkeit und längstens so lange, wie dies zur Erfüllung der Verarbeitungszwecke erforderlich ist, fort.

_____ _____

Ort, Datum Unterschrift Schülerin/Schüler

_____ _____

Ort, Datum Unterschrift Personensorgeberechtigte/r
(bei Minderjährigen)