

Data Protection Policy Nelson Mandela School

Since May 25th 2018 the General Data Protection Regulation (GDPR) is the new framework for data protection laws. The GDPR is designed to harmonise data privacy laws across Europe as well as give greater protection and rights to individuals.



Ms Berit Schweiger has been appointed as data protection officer for our school. She is responsible for schools in the districts Charlottenburg-Wilmersdorf and Steglitz-Zehlendorf and can be reached at: berit.schweiger@sima.schule.berlin.de Our guidelines were drawn up by the NMS IT & Media Development Group, in cooperation with Ms Schweiger.

The Nelson Mandela School, consisting of three campuses (Pfalzburger Straße 23 & 30 as well as Babelsberger Straße 24), gathers personal data for educational and organisational purposes. As per the School Data Regulation, no prior consent is required for the processing of any data that is part of the normal business of school. The school's collection and processing of data is subject to the following GDPR principles:

- **The transparency principle:** Personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject.
- **The purpose limitation principle:** personal data collected for one purpose should not be used for a new, incompatible, purpose. Further processing of personal data for archiving, scientific, historical or statistical purposes is still permitted.
- **The data minimisation principle:** personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which those data are processed.
- **The accuracy principle:** personal data must be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are either erased or rectified without delay.
- **The data retention period principle:** Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the data will be processed solely for archiving purposes in the public interest, or scientific, historical, or statistical purposes in accordance with Art.89(1) and subject to the implementation of appropriate safeguards
- **The data security principle:** personal data must be processed in a manner that ensures appropriate security of those data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **The accountability principle:** The school principal is responsible for, and must be able to demonstrate, compliance with the Data Protection Principles.

Paragraph 1 describes the expectations and regulations pertaining to educational staff members' processing of personal (student and parent) data. In this respect we also refer to the [NMS Social Media Guidelines](#) and the [communication guidelines](#) that all staff are expected to adhere to.

1.1 WhatsApp may not be used for communication between NMS employees and students. According to the new WhatsApp regulation, the minimum age for using WhatsApp is 16 years. The official communication via WhatsApp between employees and students / parents is not permitted regardless of age. If desired and explicitly approved by users, Messenger services with European servers and end-to-end encryption are preferable for communication between parents and teachers. For this purpose, the Nelson Mandela School has signed a contract with the secure Messenger Service [Wire](#).

1.2. The NMS staff use GSuite for Education, in order to communicate and collaborate. NMS has an international staff body, which is why German-only services are not ideal, as has been tried and tested by the IT & Media Development Group. NMS staff email addresses are Gmail-based and may only be used for professional purposes. Sensitive student information, including student's full name and surname, date of birth or address, may not be shared via email. In such instances, the use of Wire (see 1.1) is advised. When students are mentioned, this may only be done in a pseudonymised manner, for instance using initials only. Anyone using an email-address with the domain nelson-mandela-schule.net has to strictly adhere to this part of the privacy policy, as part of his/her professional work requirements. Parents and guardians are offered the opportunity to register for the child's class list, after consenting to communication via GSuite.

1.3 The use of non-European based cloud solutions such as Google Drive, Google Classroom, Dropbox and Edmodo may be used between teachers and students only if the processed data relates to curricular or organisational school matters. No personal data may be shared via these non-European based cloud solutions. Students need to be allowed a pseudonymised access to services such as Edmodo.

1.4 Teachers have to process student data. Report cards and digital class books containing absences and behavioral matters as well as other other documents containing sensitive student data may only be processed using school-internal software (Untis and Magellan). The servers of Untis and Magellan are based in Europe and both companies comply with the GDPR. If no such software is applicable (for instance for the primary school and Upper Secondary), then the school Intranet (Lehrertausch folder) is used to process sensitive information. Only in cases where sensitive data, such as when writing report cards, has to be processed on personal devices, these devices are encrypted (see 1.5) and the data pseudonymised until the moment of printing.

1.5 Student performance data is stored only for the duration of a school year - Exceptions: In the upper secondary level for the duration of the course system. After the report cards have been printed and a copy stored non-electronically in the student file, the digital data is then deleted. The behavioral data of students is temporarily stored only for printing out of certificates; the data will be deleted afterwards. In addition, student-related data will have to be removed from all personal and school devices, latest one year after the student has left the classroom. Sensitive student data may only be processed on personal devices, if the principal has agreed to this in writing and only for a limited period of time. The online application (in German only) can be found here: https://www.egovschool-berlin.de/sites/default/files/antrag_pbd_lehrerpc_0.doc. These personal devices (laptop, PC, USB-stick, flash drive) will have to be protected against unauthorised access, by password or pin, up-to-date firewall, encryption of data (for instance using Adobe Acrobat) and/or virus protection programmes.

1.6 At the beginning of the school year, the class teacher or mentor receives from the secretary the current class lists as well as a class set of student personal data forms. The class teacher hands out and collects the completed student personal sheets and compares them with the class list. The student personal data forms are to be stored by the class teacher and kept in the student files (*Schülerakten*) in the office. The secretary receives the corrected class list from each class teacher. Only administrative personnel and the IT coordinator are authorized to change and save the student data in the content management system (Magellan). Class teachers keep class lists only as 'paper copy' or securely stored on the school Intranet (*Lehrertausch*). Class lists are not shared or saved in a non-European cloud service (eg Dropbox or Drive). Educational staff takes care to always log out of the school computer when leaving the classroom or IT- or Science-lab.

1.7 Parents are asked to consent to the publication of their child's photograph on the website or in any other form (school-related). For this purpose, at the beginning of the school parents and guardians fill out and sign a consent form (*Unterschriftenseite*) handed out by the class teacher or mentor. The class teacher or mentor collects the completed signature pages and stores them in the student file (*Schülerakte*) Parents must immediately inform the class teacher or mentor in case of any relevant changes. The class teacher or mentor then is required to include those changes in the consent form in the student file (*Schülerakte*) and informs the secretary accordingly, so the latter can make the necessary adjustments into the content management system (Magellan). Class teachers and subject teachers are required to always check the student files at the start of the course or school year to see which pupils are not allowed to be photographed or filmed.

1.8 The student files may never leave the office and may only be checked by authorized persons such as class teachers and mentors, subject teachers and special needs pedagogues.

Paragraph 2 describes the expectations and regulations pertaining to the processing of personal (student, parent and teacher) data by the NMS administration. In this respect we also refer to the [NMS Social Media Guidelines](#) and the [communication guidelines](#) that all NMS community members are expected to adhere to.

2.1 To ensure the safety of personal and sensitive data, the NMS administration uses a school-internal and secure VPN for data-sharing between its campuses. All data on school-based devices is stored on school-internal servers only.

2.2 Sensitive student data (eg certificates, support measures, social matters of the Jugendamt and disciplinary measures) are kept securely in the student files (Schülerakten) and may only be accessed by the relevant staff members such as secretaries, school management, class teachers and mentors. Only information that contributes to a better understanding of the student's personality and as a basis for cooperation between the school and the home is stored. The student file is maintained by the class teacher or mentor.

2.3 All personal staff data, such as name, address and date of birth, is stored safely and may only be accessed by relevant staff, such as secretaries and management.

2.4 The substitution plan contains initials only, if it is shared via Web Untis (password protected) or on the in-house monitors. The substitution plan on the NMS website is not encrypted and may not contain references to personal data, i.e. no teachers' names or initials.

2.5 Changes to student data will be processed by the office and entered in Magellan. The office (school secretary) then creates the class list spreadsheets, which are stored and updated in the local *Lehrertausch* (teacher exchange) folder, where they can be accessed by the staff.

2.6 Parents and guardians use the signature page already mentioned above, to consent to the publication of their child's photograph on the website or in any other form (school-related). The secretaries use the information from the signature pages to create a summary page, with only the denials being reported.

Paragraph 3 offers guidelines and expectations for parents regarding data protection matters at NMS. In this respect we also refer to the [NMS Social Media Guidelines \(2017\)](#) and the [communication guidelines](#) that all staff, students and parents are expected to adhere to.

3.1 When parents register their child at the Nelson Mandela School, they will, among others, be asked by the secretary to consent to the publication of their child's photograph on the website or in any other form. For this purpose, parents are required to fill out and sign a consent form at the beginning of the school term, as well as a student personal data form. Both forms will be handed out by the class teacher (or by the secretary in Flex 1 or in case the student starts school in the middle of the school year) and will have to be filled out and handed back to the class teacher or mentor. In case of any changes regarding personal data (such as change of address, corrections in name etc) or consent, parents and guardians are required to inform the class teacher immediately.

3.2. When parents sign up for the class email lists they agree to the terms detailed upon registration. Matters containing personal and sensitive data should not be shared via email, but rather an appointment should be made to discuss matters in person or on the phone, or using encrypted communication channels, such as Wire.

3.3 The NMS Website, the Buzz Newsletter, the Förderverein (NMS Friends) and the GEV are very relevant to the school, yet serve no direct educational purposes. Their compliance with the GDPR is explained here: <https://www.nelson-mandela-schule.net/de/recht-datenschutz.html>.

3.4. Teachers, parents and students adhere to the principles mentioned in this policy, as well as to the [NMS Social Media Guidelines](#) and the [communication guidelines](#).

Datenschutzrichtlinien Nelson Mandela Schule

Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO) unmittelbar anzuwenden. Die Datenschutz-Grundverordnung (DS-GVO) zielt darauf ab, die Datenschutzgesetze in Europa zu harmonisieren und dem Einzelnen einen besseren Schutz und größere Rechte zu gewähren.



Als Datenschutzbeauftragte für unsere Schule wurde Frau Berit Schweiger bestellt. Sie ist verantwortlich für Schulen in den Bezirken Charlottenburg-Wilmersdorf und Steglitz-Zehlendorf. Sie ist erreichbar unter:

berit.schweiger@sima.schule.berlin.de

Diese Richtlinien wurden von der NMS IT/Medien Entwicklungsgruppe in Zusammenarbeit mit Frau Schweiger aufgestellt.

Die Nelson Mandela Schule, bestehend aus drei Standorten (Pfalzburger Straße 23 & 30 sowie Babelsberger Straße 24), sammelt personenbezogenen Daten für Bildungs- und Organisationszwecke. Für die Verarbeitung von Daten, in der Schuldatenverordnung geregelt ist, ist keine vorherige Zustimmung (*consent*) erforderlich. Die Erhebung und Verarbeitung von Daten durch die Schule unterliegt den folgenden DSGVO-Grundsätzen:

Grundsatz der Transparenz: Personenbezogene Daten müssen in Bezug auf die betroffene Person rechtmäßig und transparent verarbeitet werden.

Grundsatz der Zweckbindung: Zu einem bestimmten Zweck erhobene personenbezogene Daten sollten nicht für einen neuen, unvereinbaren Zweck verwendet werden. Die Weiterverarbeitung personenbezogener Daten zu archivarischen, wissenschaftlichen, historischen oder statistischen Zwecken ist weiterhin gestattet.

Grundsatz der Datenminimierung: personenbezogene Daten müssen angemessen, relevant und auf das beschränkt sein, was für die Zwecke, für die diese Daten verarbeitet werden, erforderlich ist.

Grundsatz der Richtigkeit: Die personenbezogenen Daten müssen korrekt sein und erforderlichenfalls auf dem neuesten Stand gehalten werden. Jeder Schritt muss unternommen werden, um sicherzustellen, dass unrichtige persönliche Daten unverzüglich gelöscht oder berichtigt werden.

Grundsatz der Datenspeicherfristen: Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für das Erreichen des Verarbeitungszwecks erforderlich ist. Personenbezogene Daten können für längere Zeiträume gespeichert werden, sofern die Daten ausschließlich zu Archivierungszwecken im öffentlichen Interesse oder zu wissenschaftlichen, historischen oder statistischen Zwecken gemäß Artikel 89 Absatz 1 und vorbehaltlich der Durchführung geeigneter Schutzmaßnahmen verarbeitet werden.

Grundsatz der Datensicherheit: Personenbezogene Daten müssen so verarbeitet werden, dass eine angemessene Sicherheit dieser Daten, einschließlich des Schutzes vor unbefugter oder rechtswidriger Verarbeitung und vor unbeabsichtigtem Verlust, Zerstörung oder Beschädigung, durch geeignete technische oder organisatorische Maßnahmen gewährleistet ist.

Grundsatz der Rechenschaftspflicht: der Schulleiter ist für die Einhaltung der Datenschutzgrundsätze verantwortlich und muss diese nachweisen können.

*Absatz 1 beschreibt die Erwartungen und Vorschriften für die Verarbeitung personenbezogener Daten durch das pädagogische Personal. In diesem Zusammenhang verweisen wir auch auf die [NMS Social Media Guidelines](#) und die [Kommunikationsrichtlinien](#), die von allen Mitarbeiter*innen eingehalten werden.*

1.1 WhatsApp darf für die Kommunikation zwischen NMS-Mitarbeiter*innen und Schüler*innen nicht verwendet werden. Laut der neuen Whatsapp-Regeln liegt das Mindestalter für die Nutzung von WhatsApp bei 16 Jahren. Die dienstliche Kommunikation zwischen Mitarbeitern und Schülern/Eltern ist unabhängig vom Alter nicht zulässig. Wenn gewünscht und von den Nutzer*innen ausdrücklich zugestimmt, sind für die Kommunikation zwischen Eltern und Lehrer*innen Messenger-Dienste mit europäischen Servern und Ende-zu-Ende-Verschlüsselung vorzuziehen. Die Nelson Mandela Schule hat für diesen Zweck einen Vertrag mit dem sicheren Messenger Service [Wire](#) abgeschlossen.

1.2. Die Mitarbeiter*innen des NMS verwenden G-Suite for Education, zum Kommunizieren und Zusammenzuarbeiten. NMS hat eine internationale Mitarbeiterschaft, weshalb Deutschsprachige Anbieter nicht ideal sind, wie es die IT/Medien Entwicklungsgruppe erprobt hat. Die E-Mail-Adressen der NMS-Mitarbeiter basieren auf G-Mail und dürfen nur für berufliche Zwecke verwendet werden. Empfindliche Informationen über Schüler*innen, einschließlich vollständiger Name und Vorname des Schülers, Geburtsdatum oder Adresse, dürfen nicht per E-Mail weitergegeben werden. In diesen Fällen empfehlen wir die Nutzung von Wire. Wenn Schüler*innen erwähnt werden, darf dies nur in einer pseudonymisierten Weise geschehen, beispielsweise mit Initialen. Wer eine E-Mail-Adresse mit der Domain *nelson-mandela-schule.net* verwendet, muss sich im Rahmen seiner beruflichen Anforderungen strikt an diesen Teil der Datenschutzerklärung halten. Den Erziehungsberechtigten wird die Möglichkeit geboten, sich für die Klassenliste des Kindes anzumelden, nachdem man den Kommunikationsweg über GSuite zugestimmt hat.

1.3 Die Verwendung von außereuropäischen Cloud-Lösungen wie Google Drive, Google Classroom, Dropbox und Edmodo darf nur dann durch Lehrer*innen und Schüler*innen verwendet werden, wenn sich die verarbeiteten Daten auf schulische oder organisatorische Angelegenheiten beziehen. Über diese außereuropäischen Cloud-Lösungen dürfen keine personenbezogenen Daten weitergegeben werden. Schüler*innen sollen zu Diensten wie Edmodo nur einen pseudonymisierten Zugang haben.

1.4 Schülerdaten werden durch Lehrkräfte verarbeitet. Dabei handelt es sich zum Beispiel um Zeugnissen und Einträge ins digitalen Klassenbuch, so wie Absenzen und Verhaltensauffälligkeiten, sowie andere Dokumente mit sensiblen Schülerdaten. In der Sekundarstufe I dürfen diese Einträge nur mittels schulinterner Software (Untis und Magellan) verarbeitet. Die Server von Untis und Magellan haben ihren Sitz in Europa und beide Unternehmen halten die DS-GVO ein. Wenn keine solche Software zur Verfügung steht (z. B. für die Grundschule und die Sekundarstufe II), werden lokale Schulgeräte zur Verarbeitung sensibler Informationen verwendet. Dazu wird das schulische Intranet benutzt („Lehrertausch Folder“) Nur in Fällen, in denen sensible Daten, wie Zeugnisse, auf persönlichen Geräten verarbeitet werden müssen, werden diese Geräte verschlüsselt und die Daten pseudonymisiert bis zum Zeitpunkt des Druckens (siehe 1.5).

1.5 . Die Leistungsdaten von Schülern werden nur für die Dauer eines Schuljahres gespeichert – Ausnahmen: In der in der gymnasialen Oberstufe für die Dauer des Kurssystems. Nach dem Zeugnisausdruck werden sie nicht-elektronisch dokumentiert und dann gelöscht. Die Verhaltensdaten von Schülern werden nur zum Ausdrucken von Zeugnissen vorübergehend gespeichert; die Daten werden danach gelöscht. Darüberhinaus werden die personenbezogenen Daten der Schülerinnen und Schüler spätestens ein Jahr, nachdem die Lehrkraft die/den Schüler abgegeben hat, gelöscht."Schülerdaten dürfen nur dann auf persönlichen Geräten verarbeitet werden, nachdem der Schulleiter dieses schriftlich genehmigt hat (Der Antrag und weitere Infos findet man hier: https://www.egovschool-berlin.de/sites/default/files/antrag_pbd_lehrerpc_0.doc) - und nur für einen begrenzten Zeitraum (vgl. oben). Diese persönlichen Geräte (Laptop, PC, USB-Stick, Flash-Laufwerk) müssen vor unbefugtem Zugriff geschützt werden, zB durch Passwort oder Pin, aktueller Firewall, Verschlüsselung der Daten (z. B. mit Adobe Acrobat) und / oder Viren-Schutzprogramme.

1.6 Der/die Klassenlehrer*in erhält am Anfang des Jahres vom Sekretariat die aktuelle Klassenlisten, sowie einen Klassensatz Schülerpersonalblätter. Die Klassenleitung sammelt die vollständig ausgefüllten Schülerpersonalblätter und gleicht sie ab mit der Klassenliste. Die Personalblätter werden in die Schülerbögen aufbewahrt. Das Sekretariat bekommt von jede(r) Klassenlehrer*In die berichtigte Klassenliste wieder. Nur Verwaltungspersonal und der IT-Koordinator sind berechtigt, die Schülerdaten in dem Verwaltungsmanagementsystem zu ändern und speichern. Klassenlehrer*innen führen Klassenlisten nur als 'paper copy' oder im schulinternen Netzwerk (Lehrertausch). Klassenlisten werden nicht in einem nicht-europäischen Cloud-Dienst (zB Dropbox oder Drive) freigegeben oder gespeichert. Pädagogisches Personal achtet darauf, sich immer vom Schulrechner auszuloggen beim Verlassen des Raumes.

1.7 Eltern werden gebeten, die Veröffentlichung des Lichtbildes ihres Kindes auf der Webseite oder in anderer Form zuzustimmen oder abzulehnen. Dazu wird den Eltern beim Schulanfang eine sogenannte Unterschriftenseite (*consent form*) von der Klassenleitung ausgehändigt. Die Klassenleitung sammelt die ausgefüllte Unterschriftenseite wieder ein und heftet diese im Schülerbogen ab. Änderungen müssen immer unverzüglich den Klassenlehrer*innen gemeldet werden. Diese führen die Änderungen auf der Unterschriftenseite durch und informieren der/die Sekretär*in. Klassenlehrer*innen und Fachlehrer*innen sind gehalten, immer in den Schülerbögen nachzuschauen, welche Schüler*innen nicht fotografiert werden dürfen.

1.8 Die Schülerbögen dürfen nur innerhalb des Sekretariats eingesehen werden von den berechtigten Personen, so wie Klassenleitung, Fachlehrer, Sonderpädagoge.

*Absatz 2 beschreibt die Erwartungen und Vorschriften, die sich auf die Verarbeitung personenbezogener Daten (Schüler, Lehrer und Eltern) durch die NMS-Verwaltung beziehen. In diesem Zusammenhang verweisen wir auch auf die [NMS Social Media Guidelines](#) und die [Kommunikationsrichtlinien](#), die von allen Mitarbeiter*innen eingehalten werden.*

2.1 Die Verwaltung der NMS verwendet zur Absicherung der privaten Daten ein schulinternes VPN für die gemeinsame Nutzung von Daten zwischen ihren Standorten (P23, P30, B24). Alle Daten auf schulischen Geräten werden immer nur auf schulinternen Servern gespeichert.

2.2 Sensible Schülerdaten (zB Zeugnisse, Fördermaßnahmen, soziale Belange des Jugendamtes und Disziplinarmaßnahmen) werden gesichert in dem Schülerbogen oder Sonderpädagogischen Förderbogen aufbewahrt und sind nur für die zuständigen Mitarbeiter*innen wie Sekretär*innen, Schulleitung und zuständige Klassenlehrer*innen zugänglich. Es werden nur die Informationen aufbewahrt, die zum besseren Verständnis der Persönlichkeit des Schülers beitragen und als Unterlage für die Zusammenarbeit zwischen Schule und Elternhaus dienen. Der Schülerbogen wird immer von dem/r Klassenlehrer*in geführt.

2.3 Alle persönlichen Daten der Mitarbeiter*innen, so wie Name, Adresse und Geburtsdatum werden gesichert aufbewahrt und dürfen nur vom entsprechenden Personal, wie Sekretär*innen, Verwaltungsleiter*in und Schulleiter*in, abgerufen werden.

2.4 Der Vertretungsplan enthält nur Initialen, wenn er über Untis (passwortgeschützt) oder auf den hausinternen Monitoren angezeigt wird. Der Vertretungsplan auf der NMS-Website ist nicht verschlüsselt und enthält deswegen keine Verweise auf persönliche Daten, d. H. keine Namen oder Initialen von Lehrer*innen. *(Meldung: ist nicht immer so!)*

2.5 Änderungen der Daten der Schüler*innen, werden vom Sekretariat erarbeitet und in Magellan eingegeben. Das Sekretariat erstellt daraus die Klassenlisten, die nur in dem lokalen 'Lehrertausch' Folder gespeichert werden.

2.6 Eltern stimmen, mittels der oben schon genannte Unterschriftenseite, die Veröffentlichung des Lichtbildes ihrer Kinder zu (oder lehnen diese ab). Die Sekretär*innen benutzen die Informationen aus den Unterschriftenseiten zum erstellen einer Übersichtseite, wobei nur die Ablehnungen vermeldet werden.

*Absatz 3 bietet Richtlinien und Erwartungen für Eltern in Bezug auf Datenschutz Angelegenheiten an der NMS. In diesem Zusammenhang verweisen wir auch auf die [NMS Social Media Guidelines](#) und die [Kommunikationsrichtlinien](#) die von allen Mitarbeiter*innen, Schüler*innen und Eltern eingehalten werden.*

3.1 Wenn Eltern ihr Kind an der Nelson Mandela Schule anmelden, werden sie u.a. von der/dem Sekretär*in gebeten, die Veröffentlichung des Lichtbildes ihres Kindes auf der Webseite oder in anderer Form zuzustimmen oder abzulehnen. Dazu wird den Eltern beim Schulanfang von der Klassenleitung eine sogenannte **Unterschriftenseite** (*consent form*) ausgehändigt, sowie ein auszufüllen **Schülerpersonalblatt**. Diese werden ausgefüllt an die Klassenleitung zurückgegeben. Im Falle einer Änderung der persönlichen Daten oder der erteilten Zustimmung im Laufe der Schulzeit, sind die Eltern gehalten, die Klassenleitung unverzüglich darüber zu informieren.

3.2. Wenn sich Eltern für die Klassen-E-Mail-Listen anmelden, stimmen sie den bei der Registrierung angegebenen Bedingungen zu. Angelegenheiten, die persönliche und sensible Daten enthalten, sollten nicht per E-Mail ausgetauscht werden, sondern es sollte ein Termin vereinbart werden, um persönliche Angelegenheiten zu besprechen. Eine Alternative ist, verschlüsselte Kommunikationsmitteln zu benutzen, so wie Wire.

3.3 Die NMS-Website, der Buzz-Newsletter, der Förderverein (NMS Friends) und die GEV sind für die Schule sehr relevant, dienen aber keinen direkten pädagogischen Zwecken. Ihre Einhaltung der DSGVO wird hier erläutert: <https://www.nelson-mandela-schule.net/de/recht-datenschutz.html>

Lehrer*innen, Eltern und Schüler*innen der NMS befolgen die in dieser Richtlinie genannten Grundsätze sowie die [Richtlinien für soziale Medien](#) und die [Kommunikationsrichtlinien](#) der Nelson Mandela Schule.