

# Dokumentenpaket Datenschutz und Nutzungsregelungen

## Digitale Schulumgebung der Gesamtschule Münster-West

|                  |                                                                                                 |
|------------------|-------------------------------------------------------------------------------------------------|
| Schule           | Gesamtschule Münster-West                                                                       |
| Adresse          | Tilbecker Str. 24-26, 48161 Münster                                                             |
| E-Mail           | gesamtschule-west@stadt-muenster.de                                                             |
| Website          | <a href="http://www.gesamtschule-muenster-west.de">www.gesamtschule-muenster-west.de</a>        |
| Schulträger      | Stadt Münster                                                                                   |
| IServ            | <a href="https://gemw.ms.de">https://gemw.ms.de</a> - lokale Installation auf einem Schulserver |
| MDM-System       | Jamf School                                                                                     |
| Lernplattform    | Scobees - <a href="https://learn.scobees.com/">https://learn.scobees.com/</a>                   |
| Schulisches WLAN | städtische WLAN-Infrastruktur / pädagogisches Netz                                              |
| Stand            | 27.08.2026                                                                                      |

## A. Datenschutzinformation nach Art. 13 und 14 DSGVO

Diese Datenschutzinformation beschreibt die Verarbeitung personenbezogener Daten in der digitalen Schulumgebung der Gesamtschule Münster-West. Sie gilt für IServ, schulische iPads/Jamf School, Scobees, schulisches WLAN sowie die damit verbundenen schulischen Apps und digitalen Lernangebote.

### 1. Verantwortliche Stelle

Verantwortlich für die Verarbeitung personenbezogener Daten im schulischen Bereich ist die Gesamtschule Münster-West, vertreten durch die Schulleitung, Tilbecker Str. 24-26, 48161 Münster, E-Mail: [gesamtschule-west@stadt-muenster.de](mailto:gesamtschule-west@stadt-muenster.de), Website: [www.gesamtschule-muenster-west.de](http://www.gesamtschule-muenster-west.de).

Der Schulträger ist die Stadt Münster. Soweit die Stadt Münster technische Systeme, Geräte, Netzwerke, Supportleistungen oder schulische Infrastruktur bereitstellt oder betreibt, erfolgt dies nach den erforderlichen Zuständigkeitsabgrenzungen und datenschutzrechtlichen Vereinbarungen.

Behördliche: Datenschutzbeauftragte:r der Schule / des Schulamtsbereichs Münster: Anton Allhoff,  
[datenschutz.ms1@bdsb.nrw.schule](mailto:datenschutz.ms1@bdsb.nrw.schule), 0251 411-2836

Zuständige Datenschutzaufsicht: Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI NRW), Kavalleriestr. 2-4, 40213 Düsseldorf, [poststelle@ldi.nrw.de](mailto:poststelle@ldi.nrw.de).

### 2. Zwecke der Verarbeitung

- Erfüllung des Bildungs- und Erziehungsauftrags, Unterrichtsvorbereitung, Unterrichtsdurchführung und Lernorganisation.
- Kommunikation innerhalb der Schulgemeinschaft, Aufgabenstellung, Abgabe und Rückmeldung.
- Bereitstellung und sichere Verwaltung schulischer Endgeräte, Apps, Benutzerkonten, WLAN-Zugänge und Lernplattformen.
- IT-Sicherheit, technische Administration, Fehlerbehebung, Missbrauchsvermeidung und Nachvollziehbarkeit bei konkreten Vorfällen.
- Schulische Organisation, individuelle Förderung, Beratung und Dokumentation, soweit hierfür eine rechtliche Grundlage besteht.

### 3. Rechtsgrundlagen

- Art. 6 Abs. 1 lit. e DSGVO in Verbindung mit §§ 120, 121 SchulG NRW, soweit die Verarbeitung zur Erfüllung schulischer Aufgaben erforderlich ist.
- § 120 Abs. 5 SchulG NRW und § 121 Abs. 1 SchulG NRW für den Einsatz digitaler Lehr- und Lernmittel, Lehr- und Lernsysteme sowie Arbeits- und Kommunikationsplattformen einschließlich Videokonferenzsystemen, soweit erforderlich.
- VO-DV I und VO-DV II für die jeweils zugelassenen Daten und Zwecke.
- Art. 32 DSGVO, soweit technische und organisatorische Sicherheitsmaßnahmen umzusetzen sind.
- Art. 6 Abs. 1 lit. a DSGVO nur bei freiwilligen Zusatzverarbeitungen, insbesondere Veröffentlichungen von Foto-, Video- oder Tonaufnahmen außerhalb der verpflichtenden schulischen Nutzung.

### 4. Betroffene Personengruppen

- Schüler/-innen, Erziehungsberechtigte, Lehrkräfte, weiteres pädagogisches und nichtpädagogisches Personal, schulische Administrator/-innen, Gäste und sonstige berechtigte Nutzer/-innen.

## 5. Eingesetzte Systeme und Datenkategorien

| System/Verfahren                        | Zweck                                                                                              | Typische Daten                                                                                                                                                        | Hinweise/Schutzmaßnahmen                                                                                                                             |
|-----------------------------------------|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| IServ (lokaler Schulserver, gemw.ms.de) | Kommunikation, Dateiablage, Aufgaben, Kalender, Gruppenarbeit, ggf. Messenger/Forum/Videokonferenz | Name, Vorname, Klasse/Kurs/Lerngruppe, Benutzerkennung, Schul-E-Mail, Rollen/Gruppen, Inhalte schulischer Kommunikation, Dateien, Aufgaben, technische Protokolldaten | Persönliche Konten, rollenbezogene Rechte, Protokolle nur technisch erforderlich und anlassbezogen auswertbar. Keine private Nutzung als Hauptzweck. |
| Schulische iPads / Jamf School          | Geräteverwaltung, App-Verteilung, Sicherheitsprofile, WLAN-/Zertifikatsprofile, Inventarisierung   | Geräte-ID/Seriennummer, Zuordnung, Benutzer-/Gruppenbezug, installierte schulische Apps/Profile, Gerätestatus, Sicherheitsstatus                                      | MDM dient der Verwaltung und Sicherheit, nicht der privaten Überwachung. Private Apple-IDs/Clouds nicht für schulische personenbezogene Daten.       |
| Scobees                                 | Lernplanung, Aufgabenorganisation, individuelle Lernbegleitung, Rückmeldung, Lernfortschritt       | Name, Klasse/Kurs, Aufgaben, Lernpläne, Rückmeldungen, Lernstände, ggf. Elternzugänge soweit eingerichtet                                                             | Nur pädagogisch erforderliche Daten eintragen. Leistungs-/Lernstandsdaten vertraulich behandeln.                                                     |
| Schulisches WLAN / Netzwerk             | Internet- und Netzzugang für Unterricht, Lernplattformen, schulische Apps und IT-Sicherheit        | Benutzerkennung/Berechtigungskennung, Gerätekennungen, IP/MAC-Adresse soweit technisch erforderlich, Anmeldezeitpunkte, Nutzungsdauer, technische Logs                | Zugang nur mit gültigen Berechtigungen. Protokollierung transparent, zweckgebunden und befristet. Nutzungsbedingungen der Stadt Münster beachten.    |
| Schulische Apps / digitale Lernangebote | Unterricht, Übung, Produktion, Präsentation, Kollaboration                                         | Nur die für die jeweilige App erforderlichen personenbezogenen Daten                                                                                                  | Vor Einsatz: Prüfung im VVT, ggf. AVV/DSFA/Einwilligung. Keine eigenmächtige Einführung durch Einzelpersonen.                                        |

## 6. Empfänger, Dienstleister und Auftragsverarbeitung

Empfänger personenbezogener Daten sind nur Stellen oder Personen, die diese Daten zur Erfüllung ihrer Aufgaben benötigen. Dazu können insbesondere Schulleitung, zuständige Lehrkräfte, schulische Administrator/-innen, Schulträger, beauftragte IT-Dienstleister, Anbieter der eingesetzten Systeme und im Einzelfall gesetzlich berechnigte öffentliche Stellen gehören.

Externe Dienstleister dürfen personenbezogene Daten nur im Rahmen datenschutzrechtlich zulässiger Vereinbarungen, insbesondere Auftragsverarbeitungsverträge nach Art. 28 DSGVO, und nur nach Weisung verarbeiten. Die jeweils aktuellen AV-Verträge, Unterauftragnehmerlisten, technischen und organisatorischen Maßnahmen sowie Ansprechpartner sind in der Datenschutz-Dokumentation der Schule abzulegen.

## 7. Drittlandübermittlungen und Cloud-Dienste

Vor Einsatz eines Systems ist zu prüfen und im VVT zu dokumentieren, ob personenbezogene Daten außerhalb der EU/des EWR verarbeitet werden oder ob Unterauftragnehmer in Drittländern beteiligt sind. Eine solche Verarbeitung darf nur erfolgen, wenn die Voraussetzungen der DSGVO erfüllt und dokumentiert sind. Für schulische personenbezogene Daten dürfen keine privaten Cloud-Konten oder privaten Messenger verwendet werden.

## 8. Protokollierung, Kontrolle und Auswertung

Protokolldaten werden nur verarbeitet, soweit dies für Betrieb, Sicherheit, Fehlerbehebung, Missbrauchsvermeidung oder Nachvollziehbarkeit technisch erforderlich ist. Eine anlasslose inhaltliche Überwachung findet nicht statt. Eine Auswertung von Protokollen oder Nutzerinhalten erfolgt nur anlassbezogen, verhältnismäßig, dokumentiert und durch die Schulleitung oder von ihr ausdrücklich beauftragte Personen.

- Typische Protokolldaten: Benutzerkennung, Gerätedaten, IP-/MAC-Adresse soweit technisch erforderlich, Anmeldezeitpunkte, Nutzungsdauer, Systemereignisse, Fehlermeldungen und sicherheitsrelevante Ereignisse.

- Bei konkretem Verdacht auf schwerwiegende Regel- oder Rechtsverstöße können erforderliche Protokolle gesichert und ausgewertet werden. Betroffene werden informiert, soweit dies rechtlich und tatsächlich möglich ist und keine Ermittlungs- oder Schutzinteressen entgegenstehen.

## 9. Speicherdauer und Löschung

Personenbezogene Daten werden gelöscht oder anonymisiert, sobald sie für den jeweiligen Zweck nicht mehr erforderlich sind und keine gesetzlichen Aufbewahrungsfristen entgegenstehen. Protokolldaten sind besonders kurz und zweckgebunden aufzubewahren; die konkrete Frist ist im VVT und im Löschkonzept festzulegen. Bei Abgang von der Schule werden Konten deaktiviert und Daten nach Maßgabe des Löschkonzepts gelöscht oder übergeben.

## 10. Rechte der betroffenen Personen

- Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Widerspruch nach Maßgabe der DSGVO.
- Recht auf Widerruf einer freiwilligen Einwilligung mit Wirkung für die Zukunft.
- Recht auf Beschwerde bei der zuständigen Datenschutzaufsichtsbehörde.
- Anfragen sind an die Schulleitung oder an die/den behördliche/n Datenschutzbeauftragte/n zu richten.

## 11. Datenschutzvorfälle

Verdacht auf Verlust, Diebstahl, unbefugten Zugriff, Fehlversand, Malware, kompromittierte Zugangsdaten oder sonstige Datenschutzverletzungen ist unverzüglich an die Schulleitung und die schulische Administration zu melden. Die Schulleitung bewertet unter Beteiligung der/des Datenschutzbeauftragten und ggf. des Schulträgers, ob eine Meldung an die Aufsichtsbehörde oder Benachrichtigung Betroffener erforderlich ist.

## B. Verbindliche Nutzungsordnung digitale Schulumgebung

### 1. Geltungsbereich

Diese Nutzungsordnung gilt für alle Nutzer/-innen der digitalen Schulumgebung der Gesamtschule Münster-West. Sie umfasst insbesondere IServ, schulische iPads, Jamf School, Scobeas, schulisches WLAN, schulische Benutzerkonten, schulische Apps, digitale Lernangebote, schulische Präsentations- und Netzwerktechnik sowie private Endgeräte, soweit diese im schulischen Kontext oder mit schulischer Infrastruktur genutzt werden.

### 2. Unterrichtlicher Gebrauch und erlaubte Nutzung

Als schulischer bzw. unterrichtlicher Gebrauch gelten Unterricht, Vor- und Nachbereitung, Recherche, Präsentationen, Aufgabenbearbeitung, Prüfungsvorbereitung, Berufsorientierung, Projektarbeit, Gremienarbeit, schulische Organisation sowie alle Nutzungen, die nach Inhalt und Zweck in einem unmittelbaren Zusammenhang mit der schulischen Arbeit stehen.

- Die digitalen Systeme werden ausschließlich für schulische Zwecke bereitgestellt.
- Ein Anspruch auf jederzeitige Verfügbarkeit, bestimmte Bandbreiten, bestimmte Geräte oder Nutzung privater Geräte besteht nicht.
- Private Nutzung ist nur erlaubt, wenn sie ausdrücklich gestattet ist und schulische Abläufe, Rechte anderer und IT-Sicherheit nicht beeinträchtigt.

### 3. Nutzungsberechtigte und Ende der Berechtigung

- Nutzungsberechtigt sind Schüler/-innen, Lehrkräfte, pädagogische Mitarbeiter/-innen und weitere durch die Schulleitung oder Administration zugelassene Personen.
- Gast- oder Austauschschüler/-innen, Praktikant/-innen und Externe erhalten nur temporäre und zweckgebundene Zugänge.
- Die Berechtigung endet bei Verlassen der Schule, Ende der Aufgabe, Entzug der Berechtigung oder Ablauf des Gastzugangs.

### 4. Aufsicht und Weisungen

Bei der Nutzung durch Schüler/-innen gelten die Weisungen der Lehrkräfte, der Schulleitung, der schulischen Aufsichtspersonen und der schulischen Administration. Die Nutzung schulischer Geräte oder privater Geräte im Unterricht kann durch die Lehrkraft erlaubt, eingeschränkt oder untersagt werden.

### 5. Persönliche Zugangsdaten und Passwörter

- Zugangsdaten sind persönlich, geheim zu halten und dürfen nicht gemeinsam genutzt oder weitergegeben werden.
- Fremde Zugangsdaten dürfen weder verwendet noch ausprobiert werden. Wer fremde Zugangsdaten erfährt, informiert unverzüglich die betroffene Person, eine Lehrkraft oder die Administration.
- Bei Verdacht auf Missbrauch sind Passwortänderung und Meldung an Klassenleitung, Lehrkraft oder Administration unverzüglich erforderlich.
- Nach der Arbeit an schulischen Geräten oder geteilten Geräten ist eine Abmeldung vorzunehmen.
- Passwörter müssen den schulischen Sicherheitsvorgaben entsprechen; einfache oder offenkundige Passwörter sind unzulässig.

## 6. Sorgfalt, Geräte und gespeicherte Daten

- Schulische Geräte sind sorgfältig zu behandeln, geschützt zu transportieren und nur mit freigegebenem Zubehör zu verwenden.
- Manipulationen an Hardware, Software, Profilen, MDM-Einstellungen, Netzwerken, Filtern, Zertifikaten oder Sicherheitsfunktionen sind untersagt.
- Installation von Software, Apps, Profilen oder Erweiterungen auf schulischen Geräten darf nur über freigegebene Verfahren erfolgen.
- Fremde Daten dürfen nicht gelöscht, verändert, kopiert, veröffentlicht oder unbrauchbar gemacht werden.
- Verlust, Beschädigung, Diebstahl, Malware-Verdacht oder ungewöhnliches Geräteverhalten sind unverzüglich zu melden.

## 7. Grundsatz der Datenminimierung

- Personenbezogene Daten dürfen nur verarbeitet, gespeichert oder geteilt werden, soweit dies für den schulischen Zweck erforderlich ist.
- Besonders sensible Daten, Leistungsdaten, Förderpläne, Beratungsdaten oder Gesundheitsdaten sind nur in den dafür vorgesehenen geschützten Systemen zu verarbeiten.
- Daten anderer Personen dürfen nicht ohne Befugnis weitergegeben, fotografiert, gefilmt, aufgenommen, kopiert oder veröffentlicht werden.
- Unnötige große Dateien, private Dateien und schulisch nicht erforderliche Datenablagen sind zu vermeiden und können nach vorheriger Prüfung gelöscht werden.

## 8. Stets unzulässige Nutzungen

- Abruf, Speicherung, Verbreitung oder Bereitstellung rechtswidriger, jugendgefährdender, gewaltverherrlichender, pornografischer, extremistischer, rassistischer, diskriminierender, beleidigender oder menschenverachtender Inhalte.
- Verletzungen von Urheberrecht, Persönlichkeitsrecht, Datenschutzrecht, Strafrecht oder Rechten Dritter.
- Hacking, Portscans, Umgehung von Schutzmaßnahmen, Einschleusen oder Verbreiten von Schadsoftware, Einsatz nicht freigegebener Tools oder Dienste.
- Anmeldung mit schulischen E-Mail-Adressen bei privaten Diensten, sozialen Netzwerken, Spieleplattformen oder kostenpflichtigen Angeboten, soweit nicht ausdrücklich schulisch freigegeben.
- Massenmails, Spam, Täuschung über Absender, Kettenbriefe, Drohungen, Mobbing, Cybermobbing oder belästigende Kommunikation.
- Vertragsabschlüsse, Bestellungen oder kostenpflichtige Dienste im Namen der Schule ohne ausdrückliche Berechtigung.
- Veröffentlichung schulischer Interna, Zugangsdaten, Unterrichtsmaterialien oder personenbezogener Daten in öffentlichen oder privaten Kanälen ohne Rechtsgrundlage.

## 9. Foto-, Video- und Tonaufnahmen

Foto-, Video- und Tonaufnahmen von Personen dürfen im Unterricht oder bei schulischen Veranstaltungen nur erstellt werden, wenn eine Lehrkraft dies für einen schulischen Zweck zulässt und die rechtlichen Voraussetzungen erfüllt sind. Heimliche Aufnahmen sind verboten. Veröffentlichungen außerhalb des Unterrichts oder der geschlossenen schulischen Lernumgebung benötigen eine gesonderte Rechtsgrundlage, in der Regel eine freiwillige Einwilligung.

## 10. Kontrollen, Maßnahmen und Verstöße

Die Schule kann die Einhaltung dieser Nutzungsordnung im Rahmen ihrer Befugnisse kontrollieren. Kontrollen erfolgen verhältnismäßig, zweckgebunden und möglichst transparent. Bei konkreten Verdachtsfällen oder Sicherheitsereignissen können Zugänge gesperrt, Protokolle gesichert, Datenbereiche geprüft und weitere Maßnahmen ergriffen werden.

- Mögliche Maßnahmen: pädagogisches Gespräch, Ermahnung, Information der Erziehungsberechtigten, Einschränkung einzelner Funktionen, zeitweiser oder dauerhafter Entzug von Zugängen, schulrechtliche Erziehungs- oder Ordnungsmaßnahmen, Schadensersatzprüfung, Einschaltung zuständiger Behörden bei schweren Rechtsverstößen.
- Die Ahndung erfolgt durch die Schulleitung bzw. nach den schulrechtlichen Zuständigkeiten.

## 11. Änderung, Bekanntgabe und Unterweisung

Diese Nutzungsordnung ist Bestandteil der schulischen Regelungen zur digitalen Schulumgebung und wird den Nutzer/-innen sowie bei Minderjährigen den Erziehungsberechtigten bekannt gegeben. Mindestens zu Schuljahresbeginn findet eine altersangemessene Unterweisung statt; diese wird dokumentiert. Änderungen werden in geeigneter Weise bekannt gemacht.

## C. IServ-Nutzungsordnung

### 1. Bereitstellung und Zweck

Die Gesamtschule Münster-West stellt IServ unter <https://gemw.ms.de> als schulische Kommunikations- und Austauschplattform bereit. IServ wird lokal auf einem Schulserver betrieben und dient insbesondere schulischer Kommunikation, Dateiablage, Aufgabenbearbeitung, Gruppenarbeit, Kalendernutzung und Organisation schulischer Abläufe.

### 2. Benutzerkonto

- Alle berechtigten Nutzer/-innen erhalten ein persönliches Konto. Das Konto darf ausschließlich von der berechtigten Person genutzt werden.
- Beim Verlassen der Schule wird das Konto deaktiviert und nach Maßgabe des Löschkonzepts gelöscht oder archiviert, soweit Aufbewahrungspflichten bestehen.
- Eigene Daten sind vor Verlassen der Schule innerhalb der vorgegebenen Frist zu sichern, soweit eine Sicherung zulässig und schulisch erforderlich ist.

### 3. E-Mail, Messenger, Foren, Kalender

- Schulische E-Mail-Adresse und Kommunikationsfunktionen dienen schulischer Kommunikation.
- Private Anmeldung bei Internetdiensten, sozialen Netzwerken, Online-Shops oder Spieleplattformen mit der Schuladresse ist unzulässig, soweit nicht ausdrücklich schulisch freigegeben.
- Massenmails, Joke-Mails, Kettenbriefe, beleidigende oder täuschende Nachrichten sind untersagt.
- Kalendereinträge und Gruppeninformationen sind nach bestem Wissen einzutragen und dürfen nicht manipuliert werden.
- Foren- oder Messengerbeiträge können bei Regelverstößen durch zuständige Moderator/-innen oder Administrator/-innen gelöscht, gesichert oder an die Schulleitung gemeldet werden.

### 4. Dateien und gemeinsame Ablagen

- Dateien dürfen nur mit schulischem Bezug gespeichert werden.
- Die Rechte anderer Personen, insbesondere Urheber- und Persönlichkeitsrechte, sind zu beachten.
- Freigaben sind sparsam zu verwenden. Vertrauliche Daten dürfen nur in dafür vorgesehenen geschützten Bereichen abgelegt werden.
- Die Schule übernimmt keine Verantwortung für privat oder regelwidrig gespeicherte Inhalte.

### 5. Videokonferenzen

- Teilnahme nur mit eigenem Konto und nur für schulische Zwecke.
- Keine Aufzeichnungen, Mitschnitte, Screenshots oder Weitergabe von Einwahldaten ohne ausdrückliche Erlaubnis und Rechtsgrundlage.
- Alle Inhalte bleiben im Kreis der Teilnehmenden.
- Die Privatsphäre im häuslichen Umfeld ist zu schützen; unbeteiligte Dritte sollen nicht zuhören oder zusehen.
- Mikrofon und Kamera werden nur nach unterrichtlicher Vorgabe genutzt.

### 6. Protokolle und Administration

IServ erstellt technisch erforderliche Protokolle. Die Auswertung erfolgt nur in begründeten Fällen, insbesondere bei Sicherheitsereignissen, Rechtsverstößen, Täuschungsversuchen oder schwerwiegenden Regelverstößen, und nur durch von der Schulleitung bestimmte Personen.

## D. iPad-Nutzungsordnung für Schüler/-innen

### 1. Zweck und Überlassung

Schulische iPads sind Lern- und Arbeitsgeräte. Sie dienen Unterricht, Aufgabenbearbeitung, Recherche, Präsentation, Zugriff auf IServ, Scobees und freigegebene Apps. Eine Nutzung außerhalb des schulischen Zwecks ist nur erlaubt, wenn sie ausdrücklich gestattet ist.

### 2. Verwaltung über Jamf School

Die iPads werden über Jamf School verwaltet. Dadurch können schulische Apps, Profile, Sicherheitsvorgaben, WLAN-Zugänge, Zertifikate und Einstellungen bereitgestellt werden. Die Verwaltung dient der Sicherheit und Funktionsfähigkeit der Geräte und nicht der privaten Überwachung der Schüler/-innen.

### 3. Umgang mit dem Gerät

- Gerät geschützt transportieren und geladen zum Unterricht mitbringen.
- Keine Profile, Apps, Sperren, Filter, Zertifikate oder Sicherheitseinstellungen entfernen, umgehen oder manipulieren.
- Gerät nicht an unberechtigte Personen weitergeben.
- Keine privaten Clouds, Messenger oder Accounts für schulische personenbezogene Daten nutzen.
- USB-Sticks und sonstige private externe Speichermedien werden an schulischen Geräten nicht genutzt. Datenaustausch erfolgt ausschließlich über freigegebene schulische Systeme (z. B. IServ) oder andere von der Schule freigegebene Wege.
- Verlust, Diebstahl, Beschädigung oder Funktionsstörungen sofort melden.

### 4. Private Daten auf schulischen iPads

Schulische iPads sind grundsätzlich schulische Arbeitsmittel. Private Daten sollten dort nicht gespeichert werden. Bei Rückgabe, Reparatur, Neuvergabe oder Sicherheitsvorfällen kann das Gerät ohne Sicherung privater Daten zurückgesetzt werden.

## E. Nutzung dienstlicher durch Lehrkräfte und Personal

### 1. Dienstliche Geräte

Dienstliche iPads oder sonstige dienstliche Geräte dienen Unterrichtsvorbereitung, Unterrichtsdurchführung, Kommunikation, Dokumentation und Nutzung schulischer Systeme. Personenbezogene Daten dürfen nur verarbeitet werden, soweit dies zur dienstlichen Aufgabenerfüllung erforderlich ist.

- Gerätesperre mit sicherem Code/biometrischer Sperre, soweit freigegeben.
- Keine Weitergabe an unberechtigte Personen.
- Keine Speicherung schulischer personenbezogener Daten in privaten Clouds, privaten Messenger-Diensten oder privaten Accounts.
- Regelmäßige Updates und unverzügliche Meldung von Verlust, Diebstahl, Malware-Verdacht oder Sicherheitsvorfällen.
- Besondere Sorgfalt bei Leistungsdaten, Förderplänen, Beratungsdaten, Gesundheitsdaten und sonstigen sensiblen Informationen.

## F. WLAN-Nutzungsordnung

### 1. Zweck und Zugang

Das schulische WLAN dient der schulischen Internet- und Netzwerkverbindung. Es ist kein allgemeiner privater Internetzugang. Zulässig sind insbesondere Unterricht, Recherche, ISev, Scobees, schulische Apps, digitale Lernmaterialien und schulische Kommunikation.

- Zugang nur für berechtigte Nutzer/-innen mit gültigen Zugangsdaten, verwalteten Geräten oder anderen freigegebenen Verfahren.
- Private Geräte dürfen nur genutzt werden, wenn die Schule dies erlaubt. Ein Anspruch auf Nutzung privater Geräte im WLAN besteht nicht.
- Die jeweils gültige Nutzungsordnung der Stadt Münster für WLANs an städtischen Schulen gilt ergänzend und ist bei WLAN-Zugang zur Kenntnis zu geben bzw. bestätigen zu lassen.

### 2. Pflichten der Nutzer/-innen

- Das WLAN darf nur bestimmungsgemäß, rechtmäßig und schulbezogen genutzt werden.
- Zugangsdaten dürfen nicht weitergegeben werden.
- Jugendschutzfilter, Sperren und Sicherheitsmaßnahmen dürfen nicht umgangen werden.
- Private Endgeräte müssen in einem zumutbar sicheren Zustand sein, insbesondere mit aktuellem Betriebssystem, Gerätesperre und ohne erkennbare Schadsoftware.
- Missbräuchliche oder ungewollte Nutzung eines Endgeräts im WLAN ist unverzüglich der Schule zu melden.

### 3. Protokollierung im WLAN

Bei der WLAN-Nutzung können technisch erforderliche Daten verarbeitet werden, insbesondere Benutzer-/Berechtigungskennung, IP-Adresse, MAC-Adresse bzw. Geräteerkennung, Anmeldezeitpunkt, Nutzungsdauer, Systemereignisse und gegebenenfalls Einlog- bzw. Verbindungsdaten. Die konkrete Verarbeitung, Verantwortlichkeit, Speicherdauer und Auswertung sind im VVT und in der städtischen WLAN-Nutzungsordnung zu dokumentieren.

### 4. Verfügbarkeit und Einschränkungen

Die Schule bzw. der Schulträger kann den WLAN-Zugang aus pädagogischen, technischen, rechtlichen oder sicherheitsrelevanten Gründen einschränken, sperren oder zeitweise abschalten. Mindestbandbreite, Störungsfreiheit und Verfügbarkeit werden nicht garantiert.

## G. Scobees-Nutzungsordnung

### 1. Zweck

Die Gesamtschule Münster-West nutzt Scobees unter <https://learn.scobees.com/> zur Lernplanung, Aufgabenorganisation, individuellen Lernbegleitung, Rückmeldung und Dokumentation von Lernfortschritten.

### 2. Nutzung durch Schüler/-innen

- Nur eigene Zugangsdaten verwenden.
- Aufgaben eigenständig und ehrlich bearbeiten.
- Rückmeldungen respektvoll formulieren.
- Keine fremden Inhalte löschen, verändern oder kopieren.
- Keine personenbezogenen Daten anderer unbefugt hochladen oder veröffentlichen.

### 3. Nutzung durch Lehrkräfte

- Scobees nur für pädagogisch erforderliche Planung, Begleitung und Rückmeldung nutzen.
- Leistungs- und Lernstandsdaten vertraulich behandeln.
- Rückmeldungen sachlich, pädagogisch angemessen und auf das Erforderliche beschränken.
- Keine Daten aus Scobees in private Speicher, private Messenger oder private Accounts übertragen.

## H. IT-Sicherheits- und Betriebskonzept - Mindestregelungen

Dieser Abschnitt beschreibt die organisatorischen Mindestregelungen, die für die Prüfung der Datenschutz- und IT-Sicherheit der digitalen Schulumgebung nachweisbar sein sollen. Die technischen Detailkonzepte des Schulträgers und der Dienstleister bleiben unberührt und sind in der Datenschutz-Dokumentation abzulegen.

### 1. Rollen- und Berechtigungskonzept

| Rolle                                  | Typische Berechtigungen                                                                                         | Prüfregel                                                                                                               |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| Schüler/-innen                         | Eigenes Konto, eigene Kurse/Lerngruppen, zugewiesene Aufgaben, eigene Dateien, freigegebene Kommunikationsräume | Nur eigene/zugewiesene Daten. Keine Einsicht in fremde Konten oder Verwaltungsdaten.                                    |
| Lehrkräfte                             | Eigene Kurse, Lerngruppen, Aufgaben, Rückmeldungen, pädagogisch erforderliche Kommunikations- und Dateibereiche | Zugriff nur für eigene Aufgabenerfüllung. Keine Vorratsablagen sensibler Daten auf Schülergeräten.                      |
| Klassenleitungen / Beratungsfunktionen | Erweiterte pädagogisch erforderliche Zugriffe auf die eigenen Klassen bzw. Zuständigkeitsbereiche               | Erforderlichkeit prüfen und regelmäßig entziehen.                                                                       |
| Schulleitung                           | Schulorganisatorisch und rechtlich erforderliche Zugriffe, Freigabe von Verfahren, Umgang mit Vorfällen         | Zugriffe dokumentieren und auf Erforderlichkeit beschränken.                                                            |
| Administrator/-innen                   | Technische Administrationsrechte in IServ, Jamf, WLAN/Netzwerk, Scobees soweit beauftragt                       | Adminverpflichtung, Protokollierung, keine Zweckänderung, Vier-Augen-Prinzip bei sensiblen Eingriffen nach Möglichkeit. |
| Schulträger / IT-Dienstleister         | Betrieb, Wartung, Support, Sicherheit der bereitgestellten Infrastruktur                                        | AVV/Zuständigkeitsabgrenzung, Weisungsbindung, Rollenklärung.                                                           |
| Erziehungsberechtigte                  | Nur eingerichtete Elterninformationen oder freiwillige Elternzugänge                                            | Keine automatische Einsicht in Schülerarbeitsbereiche ohne geregelten Zweck.                                            |
| Gäste / Externe                        | Nur temporäre, eng begrenzte Zugänge, soweit erforderlich                                                       | Ablaufdatum, kein Zugriff auf schulinterne Datenbereiche.                                                               |

### 2. Netzwerk- und WLAN-Sicherheit

- Trennung von Verwaltungsnetz, pädagogischem Netz, Lehrkräfte-/Personalzugängen, Schülerzugängen, Gast-/BYOD-Zugängen und administrativen Zugängen, soweit technisch möglich und mit dem Schulträger abgestimmt.
- Persönliche oder gerätebezogene Authentifizierung statt gemeinsam genutzter Sammelpasswörter, soweit technisch bereitgestellt.
- Zugriff auf Verwaltungsdaten, Leistungsdaten, Förderdaten und sensible Informationen nur über dafür vorgesehene geschützte Systeme und Rollen.
- Jugendschutz- und Sicherheitsfilter nach pädagogischem und technischem Konzept.
- Regelmäßige Überprüfung von WLAN-Zugängen, Gastzugängen und nicht mehr benötigten Berechtigungen.

### 3. Endgeräte- und App-Management

- Schulische iPads und weitere schulische mobile Geräte werden inventarisiert und über MDM verwaltet.
- Apps und Dienste werden nur nach schulischer Freigabe eingesetzt; neue Apps sind vor dem Einsatz datenschutzrechtlich und pädagogisch zu prüfen.
- Updates, Sicherheitsprofile, Gerätesperren und Löschmöglichkeiten sind Bestandteil der Gerätekonfiguration.
- Rückgabe, Defekt, Verlust, Austausch und Neuvergabe werden dokumentiert.

### 4. Administration und Support

- Administrative Rechte werden nur nach Beauftragung vergeben und regelmäßig überprüft.
- Administratoren verpflichten sich schriftlich auf Vertraulichkeit, Zweckbindung und sparsame Ausübung administrativer Rechte.
- Fernwartung und Support erfolgen nur nach geregelter Verfahren, soweit möglich mit Kenntnis der betroffenen Nutzer/-innen und dokumentierter Berechtigung.
- Standardkonten und Administrationskonten werden getrennt genutzt.

## 5. Protokollierung, Backup und Wiederherstellung

- Protokolle dienen Betrieb, Sicherheit und Nachvollziehbarkeit konkreter Vorfälle; Umfang und Fristen sind im VVT/Löschkonzept festgelegt.
- Backups werden nach dem Konzept des Schulträgers bzw. Dienstleisters erstellt und gegen unbefugten Zugriff geschützt.
- Wiederherstellung, Zurücksetzen von Geräten und Löschung erfolgen nach definierten Verfahren.

## 6. Vorfallmanagement

- Meldeweg: Nutzer/-in -> Lehrkraft/Klassenleitung/Administration -> Schulleitung -> Datenschutzbeauftragte/r/Schulträger/IT-Dienstleister je nach Vorfall.
- Typische Vorfälle: verlorenes Gerät, kompromittiertes Passwort, Fehlversand, unbefugte Veröffentlichung, Malware, ungewöhnliche Logins, Datenverlust, unbefugte Einsicht.
- Bewertung und Maßnahmen werden dokumentiert. Meldepflichten nach DSGVO werden fristgerecht geprüft.

# I. Verzeichnis der Verarbeitungstätigkeiten und Datenschutz-Dokumentation

Die Schule führt ein Verzeichnis der Verarbeitungstätigkeiten (VVT). Die konkrete Schuldatei muss alle eingesetzten Systeme, Anwendungen und Apps enthalten. Dieses Dokument ersetzt das VVT nicht, sondern liefert Textbausteine und eine prüfbare Zusammenfassung für die digitale Schulumgebung.

| Pflichtpunkt                           | Umsetzung im Dokument                                                        | Vor Beschluss zu prüfen/ergänzen                                                                                  |
|----------------------------------------|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| VVT Art. 30 DSGVO                      | Anlage mit Systemübersicht und Datenkategorien enthalten                     | VVT Teil I der Schule mit konkreten Systemen/Apps, Löschfristen, Empfängern, AVV-Status aktualisieren             |
| Datenschutzhinweise Art. 13/14 DSGVO   | Abschnitt A enthält Zwecke, Rechtsgrundlagen, Empfänger, Rechte, Löschung    | Kontaktdaten behördliche:r Datenschutzbeauftragte:r und Aufsichtsbehörde final einsetzen                          |
| AV-Verträge / Zuständigkeitsabgrenzung | Abschnitt A und Anlage nennen Schulträger, Dienstleister, IServ/Jamf/Scobeas | AVV mit Stadt Münster/Support/Jamf/Scobeas/sonstigen Dienstleistern ablegen; Unterauftragnehmer prüfen            |
| Einwilligungsprozesse                  | Pflichtnutzung von freiwilligen Zusatzverarbeitungen getrennt                | Einwilligungen nur für freiwillige Foto/Video/Öffentlichkeitsarbeit/Zusatzangebote nutzen; Widerrufe verwalten    |
| TOM / Sicherheitskonzept               | Abschnitt H beschreibt Mindestmaßnahmen                                      | Technische Details mit Schulträger abgleichen: WLAN-Segmente, Authentifizierung, Filter, Backups, Patchmanagement |
| Admin-Sensibilisierung                 | Adminverpflichtung als Formular enthalten                                    | Alle Admins jährlich/bei Rechtevergabe verpflichten und dokumentieren                                             |
| WLAN Stadt Münster                     | Städtische Nutzungsordnung eingebunden                                       | Gültige städtische Fassung als Anlage/Link bereitstellen und bei Login sichtbar machen                            |

## J. Lösch- und Berechtigungskonzept

Zugriffe werden rollenbezogen vergeben. Jede Person erhält nur die Rechte, die für ihre schulische Aufgabe erforderlich sind. Rechte werden regelmäßig und bei Wechsel der Rolle überprüft. Nicht mehr benötigte Rechte werden entzogen.

| Anlass                            | Maßnahme                                                                                                                              | Frist/Verantwortung                                                                     |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Schulwechsel / Abgang Schüler/-in | Konto deaktivieren, Datenübergabe ermöglichen, anschließend löschen/anonymisieren soweit nicht aufbewahrungspflichtig                 | Nach Löschkonzept; Verantwortlich: Schule/Administration                                |
| Ende Schuljahr / Kursende         | Kursräume, Aufgaben, geteilte Dateien und Gruppenmitgliedschaften prüfen, archivieren oder löschen                                    | Jährliche Prüfung                                                                       |
| Rückgabe / Austausch iPad         | Gerät zurücksetzen, Zuordnung und Profile entfernen, Bestandsliste aktualisieren                                                      | Bei Rückgabe / Neuvergabe                                                               |
| Wechsel / Ausscheiden Personal    | Rechte entziehen, dienstliche Daten übergeben oder löschen, private Gerätegenehmigungen prüfen                                        | Unverzüglich nach Kenntnis                                                              |
| Protokolldaten ohne Vorfall       | Nur technisch erforderliche Logs vorhalten und nach festgelegter kurzer Frist löschen                                                 | Regelfrist im VVT konkret festlegen, z. B. 30 Tage soweit technisch/vertraglich passend |
| Verdacht auf Regel-/Rechtsverstoß | Erforderliche Logs sichern, Schulleitung einbinden, Zugriff dokumentieren, nach Abschluss löschen soweit nicht aufbewahrungspflichtig | Anlassbezogen, verhältnismäßig                                                          |
| Ende Admin-Tätigkeit              | Adminrechte entziehen, Verpflichtung/Übergabe dokumentieren, Passwörter/Keys/Zertifikate prüfen                                       | Unverzüglich                                                                            |

## O. Quellen und Arbeitsgrundlagen

- Schulgesetz NRW, insbesondere §§ 120 und 121 SchulG NRW.
- VO-DV I und VO-DV II, insbesondere Vorgaben zu dienstlichen Geräten, schulischen Netzwerken, privaten Geräten von Lehrkräften und Protokolldaten.
- Dienstanweisung für die automatisierte Verarbeitung personenbezogener Daten in der Schule.
- Leitfaden „Schule datenschutzkonform aufstellen“, Bezirksregierung Münster, Stand 20.08.2024.
- Nutzungsordnung der Stadt Münster für die WLANs an den städtischen Schulen, Stand 26.05.2020.