STADT HALLE WESTFALEN
DER BÜRGERMEISTER

Name Schüler*in:

Nutzungsbedingungen für die Ausleihe von mobilen Endgeräten durch Schüler*innen

Das mobile Endgerät wird der/dem Schüler*in im Rahmen des DigitalPakts Schule Sofortausstattungsprogramm und durch finanzielle Mittel der Stadt Halle (Westf.) (Schulträger) zur Verfügung gestellt. Bei nicht volljährigen Schüler*innen erfolgt dies auf den Namen der erziehungsberechtigten Person(en). In diesen Fällen sollten die Nutzungsbedingungen vor Leistung der Unterschrift zusammen mit der/den erziehungsberechtigten Person(en) detailliert gelesen werden. Unklarheiten sind mit der in der Schule verantwortlichen Person abzusprechen. Die Kontaktdaten sind dem Schulsekretariat bekannt.

1. Geltungsbereich

Die Nutzungsbedingungen gelten für die Nutzung der von der Stadt Halle (Westf.), nachfolgend Schulträger genannt, zur Verfügung gestellten mobilen Endgeräte für die Schüler*innen an der **Gesamtschule Halle**. Die Adresse des Schulträgers lautet: Stadt Halle (Westf.), Der Bürgermeister, Abteilung 2.1 Schule, Ravensberger Str. 1, 33790 Halle (Westf.).

2. Ausstattung

Der Schulträger stellt jeweils die folgende Ausstattung als mobiles Endgerät zur Verfügung: **Apple iPad**

Das mobile Endgerät, zur Verfügung gestelltes Zubehör sowie der Zustand bei Übergabe der Ausstattung werden in der Anlage 1 genau beschrieben.

3. Leihdauer

Die Ausleihe beginnt mit der Ausgabe des mobilen Endgerätes und endet am _____.

Sofern die/der Schüler*in vor dem Ende der Ausleihe die **Gesamtschule Halle** verlassen sollte, so endet die Zeit der Ausleihe mit Ablauf des letzten Schultages. Die/Der Schüler*in hat das mobile Endgerät nach Ablauf der Ausleihe innerhalb von drei Schultagen in einem ordnungsgemäßen Zustand zurückzugeben.

4. Zweckbestimmung der Nutzung der mobilen Endgeräte

Das mobile Endgerät wird der/dem Schüler*in nur für schulische Zwecke zur Verfügung gestellt. Für die Einhaltung der Zweckbestimmung ist die/der Schüler*in selbst und bei nicht volljährigen Schüler*innen ist/sind die erziehungsberechtigte(n) Person(en) verantwortlich.

5. Ansprüche, Schäden und Haftung

Das mobile Endgerät bleibt auch während der Ausleihe Eigentum des Schulträgers und ist während der Ausleihe pfleglich zu behandeln und vor Diebstahl, Verlust oder Beschädigung bestmöglich zu schützen.

Der Diebstahl, Verlust oder die Beschädigung des mobilen Endgerätes bzw. des Zubehörs sind unverzüglich dem Schulsekretariat anzuzeigen. Das Schulsekretariat informiert darüber umgehend die in der Schule verantwortliche Person und den Schulträger. Bei einem vermuteten Diebstahl des mobilen Endgerätes erfolgt eine Standortlokalisierung und in der Regel auch eine Strafanzeige bei der Polizei. Letzteres gilt auch für vorsätzliche Beschädigungen des mobilen Endgerätes bzw. des Zubehörs.

Bei vorsätzlichen oder grob fahrlässigen Handlungen (z.B. Entnahme des Endgerätes aus der Schutzhülle), die einen Verlust oder eine Beschädigung zur Folge haben, werden die Kosten für die Wiederbeschaffung oder die Beseitigung bei Schäden der/dem Schüler*in bzw. der/den erziehungsberechtigten Person(en) in Rechnung gestellt. Ein Anspruch auf Ersatz oder Reparatur besteht nicht.

Das mobile Endgerät und das Zubehör sind nicht über den Schulträger versichert. Der freiwillige Abschluss einer entsprechenden Versicherung obliegt der/dem Schüler*in bzw. der/den erziehungsberechtigten Person(en).

6. Nutzungsbedingungen

6.1 Verhaltenspflichten

Die/Der Schüler*in bzw. die erziehungsberechtigte(n) Person(en) ist/sind für den sicheren und rechtmäßigen Einsatz des ausgeliehenen mobilen Endgerätes verantwortlich, soweit hierauf Einfluss genommen werden kann.

Die/Der Schüler*in bzw. die erziehungsberechtigte(n) Person(en) ist/sind zur Einhaltung der geltenden Rechtsvorschriften, auch innerschulischer Art, verpflichtet. Dazu gehören insbesondere Urheber-, Jugendschutz-, Datenschutz- und Strafrecht sowie die Schulordnung. Unabhängig von der gesetzlichen Zulässigkeit ist es bei der Nutzung des mobilen Endgeräts zudem nicht gestattet, verfassungsfeindliche, rassistische, gewaltverherrlichende oder pornografische Inhalte willentlich oder wissentlich abzurufen, zu speichern oder zu verbreiten.

Die/Der Schüler*in bzw. die erziehungsberechtigte(n) Person(en) verpflichtet/verpflichten sich, jederzeit Auskunft über den Verbleib des mobilen Endgeräts sowie des Zubehörs geben zu können und diese der in der Schule verantwortlichen Person vorzuführen.

Besteht der Verdacht, dass das geliehene mobile Endgerät oder eine App von Schadsoftware befallen ist, ist dies der in der Schule verantwortlichen Person unverzüglich zu melden. Im Falle des Verdachts auf Schadsoftwarebefall darf das Gerät solange nicht genutzt werden, bis die in der Schule verantwortliche Person die Nutzung wieder freigibt.

6.2 Zugriff auf die Ausstattung

Die zur Verfügung gestellte Ausstattung darf grundsätzlich nicht - auch nicht kurzfristig - an Dritte weitergegeben oder zur Nutzung überlassen werden. Eine kurzfristige Weitergabe an andere Schüler*innen oder an Lehrkräfte ist erlaubt, soweit hierfür eine schulische oder technische Notwendigkeit besteht. Über das Vorliegen der Notwendigkeit entscheidet die jeweilige Lehrkraft im Rahmen des unterrichtlichen Kontextes.

Im öffentlichen Raum ist die Ausstattung nicht unbeaufsichtigt zu lassen. Sofern die Ausstattung ohne Aufsicht im Klassenzimmer verbleibt, so ist dieses vor dem Verlassen zu verschließen.

Das mobile Endgerät darf nicht aus der ausgehändigten Schutzhülle entfernt werden.

6.3 Grundkonfiguration zur Gerätesicherheit

Im Übergabezustand sind die Endgeräte mit technischen Maßnahmen zur Absicherung gegen Fremdzugriffe und Schadsoftware vorkonfiguriert. Die durch die Systemadministration getroffenen Sicherheitsvorkehrungen dürfen nicht deaktiviert, verändert oder umgangen werden.

Die Betriebsbereitschaft (Aufladen des Akkus, Verfügbarkeit von ausreichend Speicherplatz, Aktualisierung der Betriebssoftware (iOS-Updates), etc.) ist sicherzustellen. Damit automatische Updates auf das mobile Endgerät heruntergeladen und eingespielt werden können, muss das mobile Endgerät regelmäßig, mindestens einmal pro Woche, mit dem Internet verbunden werden. Anfragen des Betriebssystems oder von installierter Software zur Installation von Updates sind grundsätzlich zu bestätigen.

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

Im Unterricht sind alle Benachrichtigungen zu deaktivieren, um Störungen zu vermeiden.

6.4 Datensicherheit (Speicherdienste)

Daten dürfen nur auf den von der Schule freigegebenen Diensten gespeichert oder ausgetauscht werden. Daten sollen nicht ausschließlich auf dem mobilen Endgerät gespeichert werden, damit diese bei Verlust, Reparatur oder Zurücksetzung nicht verloren gehen. Der Schulträger übernimmt keine Verantwortung für einen möglichen Datenverlust, insbesondere auch nicht aufgrund von Gerätedefekten oder unsachgemäßer Handhabung.

Die/Der Schüler*in bzw. die erziehungsberechtigte(n) Person(en) ist/sind für die Sicherung der Daten und der vorgenommenen Einstellungen verantwortlich. Regelmäßige Backups sollten daher ebenfalls sichergestellt werden.

6.5 Technische Unterstützung

Die technische Unterstützung durch den Schulträger umfasst die Grundkonfiguration des mobilen Endgerätes, die Abwicklungen im Rahmen von Gewährleistungs- und Garantieansprüchen, die Vornahme von zentral gesteuerten Updates, die Bereitstellung von Apps für die schulische Nutzung sowie die Analyse des mobilen Endgerätes durch

technische Maßnahmen (z.B. Virenscanner) zur Aufrechterhaltung der Informationssicherheit und zum Schutz der IT-Systeme. Die technische Unterstützung durch die **Gesamtschule Halle** umfasst eine Einweisung in das mobile Endgerät inkl. Zubehör sowie deren Nutzung sowie die Aufnahme von Problembeschreibungen – Weitergabe von Fehlermeldungen. Apps und sonstige Software auf den mobilen Endgeräten dürfen nur von der Systemadministration installiert werden.

6.6 MDM (Mobile Device Management – Mobilgeräteverwaltung)

Der Schulträger setzt über die beauftragte Systemadministration ein MDM (Mobile Device Management – Mobilgeräteverwaltung), derzeit wird die Software ***Relution*** genutzt, zur zentralen Konfiguration der mobilen Endgeräte ein. Der Schulträger behält sich vor, die mobilen Endgeräte über die Mobilgeräteverwaltung wie folgt zu administrieren:

- Entsperrcode zurücksetzen
- Gerät sperren (Entsperrcode aktivieren)
- Übertragung von Nachrichten auf die Geräte
- automatisierte Sicherheitsupdates und Analyse der gespeicherten Daten durch technische Maßnahmen (z.B. Virenscanner)

Der Schulträger darf Konformitätsregeln (sog. Profile) erstellen, um so erforderliche Update- oder Datensicherungsbedarfe oder Verstöße, etwa in Bezug auf das nicht-autorisierte Entfernen bestehender Nutzungsbeschränkungen festzustellen.

Voraussetzung für die Einrichtung des mobilen Endgerätes und des MDM durch den Schulträger oder die Schule ist die Verarbeitung von personenbezogenen Daten der Schüler*innen. Diese müssen ihre Einwilligung zur Verarbeitung personenbezogener Daten nach Artikel 7 Datenschutz-Grundverordnung geben. **Bei Schüler*innen unter 16 Jahren ist die Einwilligung der erziehungsberechtigten Person(en) erforderlich und erfolgt mit gesonderter Erklärung, die diesem Vertrag beigefügt ist.** Die Einwilligungserklärung (Anlage 2) trägt insbesondere den Transparenz- und Informationspflichten nach Artikel 13 und Artikel 14 Datenschutz-Grundverordnung Rechnung.

Das MDM erhebt beim Einsatz des mobilen Endgeräts folgende Daten:

IP-Adresse, Datum und Uhrzeit der letzten Nutzung, installierte Anwendungen und Standort

Hinweis: Diese Funktionen lassen sich im MDM nicht deaktivieren. Die für das zentrale Management verantwortlichen Personen haben die ihnen im Zusammenhang mit ihrer Tätigkeiten bekannt gewordenen personenbezogenen Daten vertraulich zu behandeln.

Die Daten werden nicht an Dritte weitergegeben; es sei denn die Weitergabe erfolgt aufgrund einer gesetzlichen Verpflichtung (z.B. Anfragen von Strafverfolgungsbehörden). Die derzeit gültige Datenschutzerklärung des genutzten MDM ist zu finden unter https://relution.io/privacy-policy/.

6.7 Regeln für die Rückgabe

Bei der Rückgabe müssen alle persönlichen Daten von dem mobilen Endgerät entfernt werden (z.B. E-Mails, gespeicherte Daten, etc.). Alle gesetzten Passwörter und PINs müssen deaktiviert werden, damit die Systemadministration das mobile Endgerät neu einrichten kann. Das mobile Endgerät ist auf die Werkseinstellungen zurückzusetzen.

7. Anerkennung der Nutzungsbedingungen

Ich versichere, die Nutzung der Ausstattung nach bestem Wissen und Gewissen unter Anerkennung und Beachtung dieser Nutzungsbedingungen vorzunehmen.

_____

Name, Vorname *(Schüler*in oder Erziehungsberechtigte Person(en))*

_____

Ort, Datum und Unterschrift *(Schüler*in oder erziehungsberechtigte Person(en))*

Übergabe der Ausstattung durch die Gesamtschule Halle (Anlage 1)

Ausgabe am (Datum):		**Rückgabe am (Datum):**	

Daten zur Ausstattung: bitte Zutreffendes ankreuzen oder ausfüllen

Apple iPad 64 GB spacegrau	☐ Ja ☐ Nein
Seriennummer des iPads	
Apple Pencil der 1. Generation mit Lightning Adapter	☐ Ja, Seriennummer: ☐ Nein
STM-Schutzhülle, schwarz	☐ Ja ☐ Nein
Original-Netzteil (Apple)	☐ Ja ☐ Nein
Original-Ladekabel (Apple)	☐ Ja ☐ Nein
Zustand	☐ Neu/Neuwertig ☐ Gebraucht
Beschreibung der Schäden bei Übergabe (ggfls. Fotos beifügen)	☐ Nein ☐ Ja, welche:
Beschädigungen (ggfls. Fotos beifügen) oder fehlendes Zubehör bei Rückgabe	☐ Nein ☐ Ja, welche:

Bestätigung der vollständigen *Übergabe*:

Ort, Datum und Unterschrift zur Übergabe *(Schüler*in oder erziehungsberechtigte Person(en))*

Halle (Westf.),

Datum, Name und Vorname, Funktion sowie Unterschrift *(Verantwortliche Person der Gesamtschule Halle)*

Bestätigung der vollständigen *Rückgabe*:

Ort, Datum und Unterschrift zur Rückgabe *(Schüler*in oder erziehungsberechtigte Person(en))*

Halle (Westf.),

Datum, Name und Vorname, Funktion sowie Unterschrift *(Verantwortliche Person der Gesamtschule Halle)*

Einwilligung nach Art. 6 Datenschutz-Grundverordnung (DS-GVO)
für die Nutzung mobiler Endgeräte durch Schüler*innen; MDM (Anlage 2)

Verantwortliche*r:

Die Verantwortliche im Sinne der DS-GVO und anderer nationaler Datenschutzgesetze der EU-Mitgliedsstaaten sowie sonstiger datenschutzrechtlicher Bestimmungen ist der Bürgermeister der Stadt Halle (Westf.), Ravensberger Str. 1, 33790 Halle (Westf.).

Behördliche Datenschutzbeauftragte:

Die Datenschutzbeauftragte der Verantwortlichen sind Frau Ilius oder ihre Vertreterin Frau Leinfelder (Kommunales Rechenzentrum Minden-Ravensberg/Lippe, erreichbar unter 05261/252-396 oder Datenschutz@hallewestfalen.de.

Umfang der Verarbeitung personenbezogener Daten

Die Stadt Halle (Westf.) verarbeitet personenbezogene Daten der Schüler*innen grundsätzlich nur, soweit dies zur Bereitstellung von Leistungen erforderlich ist. Die Verarbeitung personenbezogener Daten der Schüler*innen erfolgt regelmäßig nur nach vorheriger Einwilligung dieser betroffenen Person. Eine Ausnahme gilt in solchen Fällen, in denen eine vorherige Einholung einer Einwilligung aus tatsächlichen Gründen nicht möglich ist oder die Verarbeitung der Daten durch gesetzliche Vorschriften gestattet ist.

Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Soweit die Stadt Halle (Westf.) für Verarbeitungsvorgänge personenbezogener Daten eine Einwilligung der betroffenen Person einholt, dient Art. 6 Abs. 1 lit. a DSGVO als Rechtsgrundlage.

Unabhängig von dieser Einwilligung kann die Verarbeitung personenbezogener Daten bereits kraft Gesetzes zulässig sein:

- Bei der Verarbeitung von personenbezogenen Daten, die zur Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, erforderlich ist, dient Art. 6 Abs. 1 lit. b DS-GVO als Rechtsgrundlage. Dies gilt auch für Verarbeitungsvorgänge, die zur Durchführung vorvertraglicher Maßnahmen erforderlich sind.
- Soweit eine Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Stadt Halle (Westf.) unterliegt, dient Art. 6 Abs. 1 lit. c DS-GVO als Rechtsgrundlage.
- Für den Fall, dass lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person eine Verarbeitung personenbezogener Daten erforderlich machen, dient Art. 6 Abs. 1 lit. d DS-GVO als Rechtsgrundlage.
- Soweit eine Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich ist, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, dient Art. 6 Abs. 1 lit. e DS-GVO als Rechtsgrundlage.
- Ist die Verarbeitung zur Wahrung eines berechtigten Interesses der Stadt Halle (Westf.) oder eines Dritten erforderlich und überwiegen die Interessen, Grundrechte und Grundfreiheiten des Betroffenen das erstgenannte Interesse nicht, so dient Art. 6 Abs. 1 lit. f DS-GVO als Rechtsgrundlage für die Verarbeitung.

Zweck der Datenverarbeitung laut Art. 5 Abs. 1 lit. b DS-GVO

Die erhobenen Daten dürfen nur für den nachstehend aufgeführten Zweck verarbeitet werden:

- Administrierung des ausgeliehenen mobilen Endgerätes sowie der darauf genutzten Software

Die Daten werden auf den Servern der Firmen gespeichert, deren Software für die Mobilgeräteverwaltung eingesetzt bzw. die mit der Mobilgeräteverwaltung beauftragt sind, und können nur von berechtigten Personen eingesehen und bearbeitet werden.

Eingesetzte Software für die Mobilgeräteverwaltung bei Herausgabe dieser Nutzungsbedingungen:

MDM Relution

Die tatsächlich gespeicherten Dateien hängen im Einzelfall davon ab, welche Software eingesetzt wird und welche Funktionen bei der Mobilgeräteverwaltung aktiviert werden. Die folgende Auflistung zeigt die dabei maximal gespeicherten Daten, wobei in vielen Fällen weniger Daten gespeichert werden:

- Benutzerinformationen: Besitzername/Anzeigename des Benutzers (der in Azure registrierte Name des Benutzers, der durch die AzureUserID identifiziert wird), Benutzerprinzipalname oder E-Mail-Adresse, Benutzer-IDs von Drittanbietern (z. B. Apple-ID)
- Hardwareinventurinformationen: Gerätename, Hersteller, Betriebssystem, Seriennummer, IMEI-Nummer, IP-Adresse, WLAN-MAC-Adresse
- Überwachungsprotokollinformationen einschließlich Daten zu folgenden Aktivitäten: Verwalten, Erstellen, Aktualisieren (Bearbeiten), Löschen, Zuweisen, Remoteaufgaben

- Supportinformationen: Kontaktinformationen (Name, E-Mail-Adresse), E-Mail-Unterhaltungen mit Mitgliedern der Supportteams, -Produktteams oder der Teams für Benutzerzufriedenheit
- Informationen zur Zugriffssteuerung: Statische Authentifikatoren (Kennwort des Kunden), Datenschutzschlüssel für Zertifikate
- Vom Administrator erstellte Daten, z. B.: (Profilnamen, Kompatibilitätsrichtlinien, Gruppen-richtlinie, PowerShell-Skripts, Branchenspezifische App, Anwendungsbestand, z.B.: App-Name, Version, App-ID, Größe, Installationspfad)

Die Gesamtliste ist abrufbar unter: https://relution.io/privacy-policy/

Daten die nicht abrufbar sind vom Administrator:

Anruf- oder Webbrowserverlauf, persönliche E-Mails, Textnachrichten, Kontakte, Kennwörter für persönliche Konten, Kalenderveranstaltungen oder Fotos (einschließlich Fotos in einer Foto-App oder Kamera)

Alle Daten liegen in Datenzentren innerhalb der Europäischen Union und unterliegen den Datenschutzgesetzen der EU. Die für die Kontoerstellung verwendeten oder in den Systemen von Jamf School gespeicherten Daten werden grundsätzlich nicht an Dritte weitergegeben.

Als Ausnahme ist der CLOUD Act zu betrachten:

„Der CLOUD Act (Clarifying Lawful Overseas Use of Data Act) ist ein US-amerikanisches Gesetz. Es verpflichtet amerikanische Internet-Firmen und IT-Dienstleister, US-Behörden auch dann Zugriff auf gespeicherte Daten zu gewährleisten, wenn die Speicherung nicht in den USA erfolgt. Dem von der Herausgabeverpflichtung betroffenen Unternehmen steht jedoch nach dem Gesetz im Einzelfall ein Widerspruchsrecht gegen die Anordnung zur Herausgabe von Daten zu, wenn der Eigentümer der Daten kein US-Bürger ist, nicht in den USA lebt und das Unternehmen durch die Herausgabe der Daten gegen ausländisches Recht (in Europa zum Beispiel die DS-GVO) verstoßen würde."

Quelle: https://de.wikipedia.org/wiki/CLOUD_Act

Datenlöschung und Speicherdauer

Die personenbezogenen Daten der Schüler*innen werden gelöscht oder gesperrt, sobald der Zweck der Speicherung entfällt, z. B. die Beendigung der Ausleihe oder Verlassen der Schule. Eine Speicherung kann darüber hinaus erfolgen, wenn dies durch den europäischen oder nationalen Gesetzgeber in unionsrechtlichen Verordnungen, Gesetzen oder sonstigen Vorschriften, denen die Stadt Halle (Westf.) unterliegt, vorgesehen wurde. Eine Sperrung oder Löschung der Daten erfolgt auch dann, wenn eine durch die genannten Normen vorgeschriebene Speicherfrist abläuft, es sei denn, dass eine Erforderlichkeit zur weiteren Speicherung der Daten für einen Vertragsabschluss oder eine Vertragserfüllung besteht.

Betroffenenrechte lt. Art. 15 – 21 DS-GVO

Sie haben ein Auskunfts-, Löschungs-, Berichtigungs-, Einschränkungs- und Widerspruchsrecht sowie das Recht auf Datenübertragbarkeit. Das Löschungs-, Einschränkungs- und Widerspruchsrecht ist insofern eingeschränkt, soweit die Daten zur Erfüllung gesetzlicher Anforderungen verarbeitet werden. Im Falle einer Einwilligung besteht das Recht, die Einwilligung jederzeit zu widerrufen. Die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung wird hiervon nicht berührt (Art. 13 Abs. 2 lit. c DS-GVO).

Bitte wenden Sie sich dazu an die Stadt Halle (Westf.), Ravensberger Staße. 1, 33790 Halle (Westf).

Beschwerde- und Fragerecht:

Für Beschwerden können sich Schüler*innen und erziehungsberechtigte Personen jederzeit an folgende Stellen wenden:

- Schulleiter*in als für den Datenschutz an der Schule zuständige Person,
- Stadt Halle (Westf.), Abteilung 2.1, Ravensberger Staße. 1, 33790 Halle (Westf.),
- Schulische*r Datenschutzbeauftragte*r beim Kreis Gütersloh (datenschutz.schulamt@kreis-guetersloh.de),
- Datenschutzbeauftragte der Stadt Halle (Westf.),
- die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (siehe https://www.ldi.nrw.de).

_____

Ort, Datum und Unterschrift *(Schüler*in oder erziehungsberechtigte Personen(en))*

Einwilligung in die Erhebung und Speicherung von personenbezogenen Daten zur Nutzung der Microsoft 365 Clouddienste (Anlage 3)

Verantwortliche*r:

Die Verantwortliche im Sinne der DS-GVO und anderer nationaler Datenschutzgesetze der EU-Mitgliedsstaaten sowie sonstiger datenschutzrechtlicher Bestimmungen ist die Gesamtschule Halle, Wasserwerkstraße 1, 33790 Halle (Westf.).

Behördliche*r Datenschutzbeauftragte*r:

Die/Der Datenschutzbeauftragte*r für das Schulamt und die Schulen des Kreises Gütersloh beim Schulamt für den Kreis Gütersloh, Herzebrocker Straße 140, 33324 Gütersloh, erreichbar unter 05241/85-1417 oder 05242/40809-232 oder datenschutz.schulamt@kreis-guetersloh.de.

1. Einwilligung

Mit der Nutzung erteile ich die Einwilligung, dass die Gesamtschule Halle zur Erstellung eines Office 365 Cloud Kontos folgende Daten an Microsoft weitergeben darf: SchülerID; Vor- und Nachname; Tag, Monat und Jahr des Geburtsdatums; schulische E-Mail-Adresse.

Microsoft speichert die Logdaten der Zugriffe auf das Konto und die Dienste und sendet Telemetriedaten zur Verbesserung der Software bei der Arbeit der Benutzer an seine Rechenzentren. Es werden keine weiteren personenbezogenen Daten in der Microsoft-Cloud gespeichert, insbesondere keine Leistungsdaten oder Verhaltens- und / oder Gesundheitsdaten.

2. Zweck der Datenspeicherung

Die Datenspeicherung und die Videokonferenzen dienen ausschließlich dem Zweck der unterrichtlichen Bereitstellung und Erklärung von Unterlagen. Die Unterlagen werden von den Kolleg*innen individuell bearbeitet und können nur durch Freigabe anderen Kolleg*innen oder Schüler*innen eingesehen werden. Im Rahmen der unterrichtlichen Arbeit werden von Seiten der Kolleg*innen Bewertungen der Schülerleistungen vorgenommen, die aber nicht über das Cloudsystem publiziert werden.

3. Speicherort und Datensicherheit

Alle Daten, die unter Verwendung des von der Schule generierten Logins in der Microsoft-Cloud gespeichert werden, liegen in Datenzentren innerhalb der Europäischen Union und unterliegen den Datenschutzgesetzen der EU. Die für die Kontoerstellung verwendeten oder in den Systemen von Microsoft gespeicherten Daten werden nicht an Dritte weitergegeben. Der Zugriff auf die Daten ist nur der/dem Nutzer*in unter Verwendung eines von ihr/ihm selbst erstellten, sicheren Kennworts möglich und den Systemadministratoren. Das Login/Authentifizierung zu den Office365 Clouddiensten geschieht durch Rechenzentren, die in den USA liegen.

„Der CLOUD Act (Clarifying Lawful Overseas Use of Data Act) ist ein US-amerikanisches Gesetz. Es verpflichtet amerikanische Internet-Firmen und IT-Dienstleister, US-Behörden auch dann Zugriff auf gespeicherte Daten zu gewährleisten, wenn die Speicherung nicht in den USA erfolgt. Dem von der Herausgabeverpflichtung betroffenen Unternehmen steht jedoch nach dem Gesetz im Einzelfall ein Widerspruchsrecht gegen die Anordnung zur Herausgabe von Daten zu, wenn der Eigentümer der Daten kein US-Bürger ist, nicht in den USA lebt und das Unternehmen durch die Herausgabe der Daten gegen ausländisches Recht (in Europa zum Beispiel die DS-GVO) verstoßen würde."

Quelle: https://de.wikipedia.org/wiki/CLOUD_Act

4. Datensicherung / Backup

Weder die Gesamtschule Halle noch Microsoft sind für die Ausfalldatensicherung der in der Cloud liegenden Daten verantwortlich. Die/Der Benutzer*in hat somit selbst sicherzustellen (z.B. durch ein Backup), dass im Falle eines Systemausfalls im Datenzentrum, keine für die/den Benutzer*in relevanten Daten verloren gehen.

5. Beendigung des Einverständnisses (automatisch bei Verlassen der Schule)

Der/Dem Nutzer*in ist bewusst, dass dies eine umgehende und unwiederbringliche Löschung der Personen und Nutzungsdaten des Office 365 Cloud Kontos zur Folge hat. Die/Der Nutzer*in hat selbst dafür Sorge zu tragen, dass vor Beendigung der Schulzugehörigkeit alle relevanten ggf. in der Cloud gespeicherten Daten gesichert wurden.

6. Widerruf

Diese Einwilligung kann für die Zukunft jederzeit widerrufen werden. Die Einwilligung kann auch teilweise widerrufen werden. Im Falle des Widerrufs dürfen personenbezogene Daten zukünftig nicht mehr für die oben (Ziff. 2 und 3) genannten Zwecke verwendet werden und sind unverzüglich zu löschen.

Der/Dem Nutzer*in ist bewusst, dass dies eine umgehende und unwiederbringliche Löschung der Personen und Nutzungsdaten des Office 365 Cloud Kontos zur Folge hat. Soweit die Einwilligung nicht widerrufen wird, gilt sie zeitlich unbeschränkt, d.h. auch über das Ende der Schulzugehörigkeit hinaus.

Die Einwilligung ist freiwillig, aus der Verweigerung der Einwilligung oder ihrem Widerruf entstehen keine Nachteile. Der Widerruf ist zu richten an die Gesamtschule Halle, Wasserwerkstraße 1, 33790 Halle (Westf.).

7. Beschwerde- und Fragerecht:

Für Beschwerden können sich Nutzer*innen und erziehungsberechtigte Personen jederzeit an folgende Stellen wenden:

- Schulleiter*in als für den Datenschutz an der Schule zuständige Person,
- Schulische*r Datenschutzbeauftragte*r beim Kreis Gütersloh (datenschutz.schulamt@kreis-guetersloh.de),
- die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (siehe https://www.ldi.nrw.de).

_____

Ort, Datum und Unterschrift *(Schüler*in oder erziehungsberechtigte Personen(en))*