

2020

# Handreichung zur Nutzung von Office 365 an Schulen

GRACE-HOPPER-GESAMTSCHULE



## INHALT

1. Vorwort .....	2
2. Einführung in die DSGVO.....	3
2.1. Allgemeine Beschreibungen und Definitionen .....	3
2.1.1. Allgemeines zur Datenschutzgrundverordnung .....	3
2.1.2. Zentrale Aussagen der DSGVO .....	3
2.1.3. Verarbeitung im Auftrag.....	3
2.1.4. Welche Gesetze sind im Zusammenhang mit IT zu beachten? .....	4
2.2. Rechte und Möglichkeiten der Aufsichtsbehörden .....	5
2.3. Datenschutz der Länder .....	6
3. Datenschutz an Schulen .....	6
3.1. Verantwortlicher .....	6
3.2. Rechtsgrundlage für die Verarbeitung.....	7
3.2.1. Rechtsgrundlage für Office 365 Education als pädagogisches System .....	7
3.2.2. Dienstvereinbarung für Lehrer und Lehrerinnen .....	7
3.2.3. Einwilligung der Nutzer .....	7
3.3. Datenschutzbeauftragter .....	7
3.4. Auftragsverarbeitung.....	8
3.5. Verzeichnis von Verarbeitungstätigkeiten und technische/organisatorische Maßnahmen.....	8
3.6. Nutzungsordnung .....	9
3.7. Zusammenfassung .....	9
4. Anhang .....	11
4.1. Abkürzungen.....	11
4.2. Links/Quellen/Normen .....	11
4.3. Muster .....	14

## I. VORWORT

Die vorliegende Handreichung bietet Bildungseinrichtungen die Möglichkeit, die nach dem 25.05.2018 nach der DSGVO geltenden Datenschutzregeln umzusetzen.

Alle Checklisten und Muster können für die täglichen Aufgaben und die Dokumentation und Umsetzung des Datenschutzes genutzt und ergänzt werden.

Die Handreichung stellt dabei keine Rechtsberatung dar und kann auch keine umfangreiche Beratung durch einen Datenschutzbeauftragten ersetzen.

Die Autoren sind über dankbar über Anmerkungen und konstruktive Kritik. Feedback bitte an eine der folgenden E-Mails:

- [feedback@cczone.de](mailto:feedback@cczone.de)
- [info@konverion.de](mailto:info@konverion.de)
- [info@drvis.de](mailto:info@drvis.de)

## 2. EINFÜHRUNG IN DIE DSGVO

### 2.1. ALLGEMEINE BESCHREIBUNGEN UND DEFINITIONEN

#### 2.1.1. ALLGEMEINES ZUR DATENSCHUTZGRUNDVERORDNUNG

Die europäische Datenschutzgrundverordnung <https://aka.ms/dsgvo-grundverordnung> regelt die automatisierte Verarbeitung von personenbezogenen Daten, also Daten, mit denen sich ein eindeutiger Bezug zu einer Person herstellen lässt. Es geht also nicht um den Schutz geistigen Eigentums. Die Kernidee ist, dass es für die Verarbeitung personenbezogener Daten einen vernünftigen, schlüssigen Grund geben muss und die Betroffenen das Recht haben, zu erfahren,

- Wer Zugriff auf die Daten hat?
- Warum der Zugriff besteht?
- Wo die Daten verarbeitet werden?
- Wie lange eine Verarbeitung erfolgt?

#### 2.1.2. ZENTRALE AUSSAGEN DER DSGVO

Artikel 1 (3) der DSGVO lautet: „Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden“. Daher ist eine Beschränkung auf Deutschland oder eine Beschränkung auf die eigenen Räumlichkeiten nicht zulässig. Damit spielt erstmals das "wo" keine Rolle, sondern nur das "wie".

Eine Bildungseinrichtung ist nach Artikel 32 DSGVO verpflichtet, darüber Auskunft geben zu können, welche Maßnahmen in technischer und organisatorischer Hinsicht getroffen wurden, um die Datenschutzbestimmungen einzuhalten. Die technischen Schutzmaßnahmen müssen „dem aktuellen Stand der Technik“ entsprechen. Diese Forderung bedeutet eine vollkommene Abkehr vom bisherigen Prinzip „my home is my castle“, welches im alten Bundesdatenschutzgesetz vertreten wurde.

Das Gesetz setzt sich erstmals mit den dramatisch wachsenden Gefahren durch technische Sicherheitslücken auseinander und verlangt den technisch bestmöglichen Schutz personenbezogener Daten in Abhängigkeit von den Nachteilen, die einer Person durch deren unbeabsichtigte Veröffentlichung entstehen können. Im Kern anerkennt die DSGVO damit, dass angesichts der Entwicklung des Internets ein adäquater Datenschutz durch eine lokale Serverinfrastruktur in aller Regel nicht mehr erbracht werden kann. Nur sehr große, professionell betriebene und entsprechend ausgestattete Rechenzentren verfügen über die Mittel, den wachsenden Bedrohungen wirksame Schutzmaßnahmen entgegensetzen zu können. Dies wiederholt im gewissen Sinne die Jahrzehnte alte Entwicklung in einem anderen Bereich: weg vom Kohle- oder Ölofen in jeder Wohnung hin zur heutigen Fernwärme. Niemand wird heute den dadurch erreichten Sicherheitsgewinn mehr bestreiten.

#### 2.1.3. VERARBEITUNG IM AUFTRAG

Wenn eine Bildungseinrichtung ihre IT nicht mehr selbst betreiben will oder soll, wer ist dann verantwortlich? Es ist wichtig zu verstehen, dass die Datenschutzverantwortung bei jedem IT-Dienst, den die Bildungseinrichtung einsetzt, zur Gänze bei der Bildungseinrichtung liegt, nicht beim Auftragsverarbeiter wie z. B. Microsoft. Bildlich gesprochen bietet Microsoft ein Fahrzeug an, das nach StVO alle Vorschriften erfüllt und zugelassen ist, aber der Fahrer ist die Bildungseinrichtung. Sie muss festlegen, warum welche personenbezogenen Daten

verarbeitet und gespeichert werden, wie lange sie gespeichert bleiben und wer Zugriff auf die Daten hat.

Für die Auswahl von IT-Dienstleistern (Auftragsverarbeiter nach Art. 28 DSGVO) gelten in der DSGVO wesentlich strengere Maßstäbe und eine Bildungseinrichtung muss konkret nachweisen können, dass die Auswahl nach objektiven datenschutzrechtlichen Kriterien erfolgt ist, z.B. durch eine Zertifizierung des Anbieters. So sind die Microsoft EU Rechenzentren nach dem Datenschutz-Standards ISO 27001 und 27018 (<https://aka.ms/compliance-angebote>) zertifiziert. Artikel 28 (1) lautet: „Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt ...“.

#### 2.1.4. WELCHE GESETZE SIND IM ZUSAMMENHANG MIT IT ZU BEACHTEN?

Grundsätzlich gibt es eine Gesetzes-Hierarchie: EU Recht wie die DSGVO geht vor Bundesrecht geht vor Landesrecht. Bei Konflikten gilt das Gesetz der übergeordneten Instanz, untergeordnete Gesetze regeln Dinge, die im übergeordneten nicht geregelt sind.

Im Gegensatz zu früher gilt die DSGVO für öffentliche und nicht öffentliche Organisationen gleichermaßen und sie ist das relevante Gesetz für alle datenschutzrechtlichen Aspekte. Die DSGVO sieht allerdings Öffnungsklauseln für den öffentlichen Dienst vor. Das neue Bundesdatenschutzgesetz und die neuen Landesdatenschutzgesetze nutzen diese zur Regelung von Gefahrenabwehr (z. B. mittels Videoüberwachung), Strafverfolgung und -vollzug und Dienstvereinbarungen. Relevant sind diese Öffnungsklauseln für öffentliche Bildungseinrichtungen in einem kleinen Teilaspekt auch deswegen, weil sie danach von der Verhängung von Geldbußen befreit werden (was derzeit in den meisten Bundesländern allerdings noch nicht umgesetzt ist).

Für eine Bildungseinrichtung gibt es außerdem die Schul- bzw. Hochschulgesetze, die datenschutzrechtliche Aspekte enthalten können wie z. B. ein generelles Werbeverbot an Schulen. Alle Landes-Schulgesetze enthalten Absätze, in denen die Verarbeitung personenbezogener Daten zum Zwecke der Erfüllung der schulischen Aufgaben geregelt ist. Auf dieses Recht zur Verarbeitung personenbezogener Daten in Schulen, das im öffentlichen Interesse liegt, bezieht sich auch die DSGVO.

##### Einsatz von IT gestütztem Unterricht

Eine staatlich anerkannte Bildungseinrichtung hat den gesetzlichen Auftrag, Lernenden eine zeitgemäße Ausbildung anzubieten. Dazu gehört in allen Fällen eine Bewertung der Leistungen des Lernenden und in vielen Fällen (wie z. B. in etlichen Schulgesetzen verankert ist) die Vermittlung moderner Medienkompetenz. Diese Fakten sind nicht ohne Weiteres mit der DSGVO verträglich. Andererseits muss jede Verarbeitung personenbezogener Daten rechtmäßig sein. Es muss also eine Rechtsgrundlage für die Verarbeitung vorliegen.

Daher ist eine wichtige Frage, wie eine Schule IT-gestützten Unterricht datenschutzkonform anbieten kann. Kurz gesagt, gibt es 2 Möglichkeiten: man kann IT-gestützten Unterricht freiwillig anbieten oder nach einem Beschluss des Schulgremiums, dem alle Gruppen einer Schule (Lehrer-, Schüler-, Eltern-Vertreter) angehören.

Freiwilliger Einsatz ist sinnvoll, wenn es um eine Pilotgruppe geht oder einen Testlauf. Der springende Punkt bei freiwilligem Einsatz ist, dass ein Betroffener jederzeit widersprechen kann. Nach einem solchen Widerspruch ist zu überlegen, ob der Testlauf noch fortgesetzt werden kann, denn ein sozialer Druck auf die Teilnehmer darf dadurch nicht entstehen. Für systematischen Einsatz von IT-gestützten Unterricht ist aber ein Beschluss zu empfehlen, den wir weiter unten im Detail erläutern und exemplarisch anführen.

## 2.2. RECHTE UND MÖGLICHKEITEN DER AUFSICHTSBEHÖRDEN

Zu den wesentlichen Aufgaben (Hauptaufgaben, gemäß Art. 57 DSGVO) der Landesdatenschutzbehörden gehören:

- Die Anwendung der DSGVO zu überwachen und durchzusetzen,
- Anfragen und Beschwerden von Betroffenen zu bearbeiten,
- Öffentliche und Nicht-Öffentliche Einrichtungen bezüglich ihrer Datenschutzpflichten zu sensibilisieren und
- Untersuchungen über die Anwendung der DSGVO durchzuführen.

Durch die DSGVO bekommt eine Aufsichtsbehörde sehr weitreichende Befugnisse (Art. 58 DSGVO). Die Befugnisse lassen sich dabei in Untersuchungs-, Abhilfe-, Genehmigungs- und Beratungsbefugnisse einteilen. Darüber hinaus kann eine Aufsichtsbehörde gemäß Art. 83 DSGVO Geldbußen verhängen, davon ist der öffentliche Bereich jedoch ausgeschlossen (§ 43 Abs. 3 BDSG).

Im Rahmen der Untersuchungsbefugnisse (Art. 58 Abs. 1 DSGVO) kann eine Aufsichtsbehörde anlassbezogene oder anlasslose Datenschutzprüfungen durchführen. Eine Datenschutzprüfung kann verschiedene Ziele verfolgen

- Beschwerdeprüfung: Ist eine Datenschutzbeschwerde eines Betroffenen begründet?
- Konzeptionsprüfung: Ist die Datenverarbeitung in der Schule ausreichend beschrieben bzw. dokumentiert?
- Angemessenheitsprüfung: Ist die DSGVO in allen wesentlichen Belangen angemessen umgesetzt und eingeführt?
- Wirksamkeitsprüfung: Ist die DSGVO in allen wesentlichen Belangen angemessen umgesetzt, eingeführt und wirksam?

Über die Abhilfebefugnisse (Art. 58 Abs. 2 DSGVO) kann eine Aufsichtsbehörde, Verantwortliche und Auftragsverarbeiter warnen und/oder von den Maßnahmen der DSGVO Gebrauch machen:

- Einhaltung der Betroffenenrechte sicherstellen
- Betroffene über Datenschutzverletzungen benachrichtigen
- Eine Verarbeitung befristet oder endgültig untersagen
- Geldbußen verhängen

Mit den Genehmigungs- und Beratungsbefugnissen (Art. 58 Abs. 3 DSGVO) sensibilisiert und berät die Aufsichtsbehörde öffentliche und nicht-öffentliche Einrichtungen und sorgt mit geeigneten Mitteln dafür, dass Datenschutzverletzungen nicht eintreten. Damit soll dem Hauptanliegen, die Einhaltung des Datenschutzes (vorbeugender Grundschutz), Rechnung getragen werden.

Eine Landesdatenschutz-/Aufsichtsbehörde ist somit für die Beratung von Verantwortlichen und Überwachung des Datenschutzes verantwortlich. Jedoch ist sie nicht befugt, eine Entscheidung für die verantwortliche Stelle zu treffen.

## 2.3. DATENSCHUTZ DER LÄNDER

Mit dem jeweilig geltenden Schulgesetz (<https://aka.ms/schulgesetze-laenderebene>) ist auch eine Rechtsgrundlage für Verarbeitung personenbezogener Daten und implizit die Nutzung einer Lehr- und Lern-Plattform gegeben. Für die 16 Bundesländer finden Sie folgend die entsprechenden Normen:

Bundesland	Öffentliche Schulen	Freie Trägerschaft
Baden-Württemberg	§ 1 SchG	§ 1 PSchG
Bayern	Art. 85 BayEUG	Art. 90 BayEUG
Berlin	§ 64 SchulG	§ 95 SchulG
Brandenburg	§ 65 BbgSchulG	§ 127 BbgSchulG
Bremen	§ 3 BremSchulG	§ 1 PrivSchG
Hamburg	§ 98 HmbSG	§ 3 HmbSfTG
Hessen	§ 83 HSchG	§ 166 HSchG
Mecklenburg-Vorpommern	§ 7 SchulG M-V	§ 116 Trägerschaft
Niedersachse	§ 31 NSchG	§ 139 NSchG
Nordrhein-Westfalen	§ 120 und 212 SchulG	§ 100 SchulG
Rheinland-Pfalz	§ 67 SchulG	§ 1 PrivSchG
Saarland	§ 20b SchoG	§ 1 PrivSchG
Sachsen	§ 63a SächsG	§ 1 SächsFrTrSchulG
Sachsen-Anhalt	§ 84a SchulG LSA	§ 14 SchulG LSA
Schleswig-Holstein	§ 4 SchulG	§ 115 SchulG
Thüringen	§ 57 ThürSchulG	§ 2 ThürSchfTG

Damit Schulen nicht von allen Nutzern eine Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO einholen müssen, ermöglicht Art. 6 Abs. 1 lit. e DSGVO im Verbund mit dem für das Land geltende Schulgesetz, personenbezogene Daten für den Einsatz von Lehr- und Lernplattformen einzusetzen. Alternativ (nur bei Privatschulen) ist die Rechtmäßigkeit dafür nach Art. 6 Abs. 1 lit. c DSGVO möglich.

## 3. DATENSCHUTZ AN SCHULEN

### 3.1. VERANTWORTLICHER

Wichtig ist, dass die als Schule immer die datenschutzrechtlich verantwortliche Stelle bleibt. Microsoft ist nur Dienstleister bzw. Auftragsverarbeiter. Somit muss die Schule die Rechtmäßigkeit

der Verarbeitung sicherstellen. Des Weiteren ist die Schule für die Umsetzung geeigneter technischer und organisatorischer Maßnahmen sowie der Betroffenenrechte verantwortlich bzw. zuständig.

## 3.2. RECHTSGRUNDLAGE FÜR DIE VERARBEITUNG

### 3.2.1. RECHTSGRUNDLAGE FÜR OFFICE 365 EDUCATION ALS PÄDAGOGISCHES SYSTEM

Rechtsgrundlagen für die Verarbeitung personenbezogener Schülerdaten auch in Office 365 Education sind zunächst die DSGVO im Verbund mit den jeweiligen Schulgesetzen und dazu erlassene Rechtsverordnungen (z.B. Beschluss der Schulkonferenz oder eine Dienstvereinbarung). Ergänzend können – je nach Bundesland und Schultyp – die Landesdatenschutzgesetze sowie das Bundesdatenschutzgesetz für die in der DSGVO nicht geregelten Details zur Anwendung kommen.

Die Verwendung einer Lehr- und Lernplattform kann durch oder aufgrund einer Verordnung (z.B. Dienstvereinbarung oder Beschluss der Schulkonferenz) vorgeschrieben werden. Denkbar ist beispielsweise die Bestimmung als Lehrmittel durch entsprechende Verordnung (gemäß Art. 6 Abs. 1 lit. c und e, Abs. 2 und 3 DSGVO).

### 3.2.2. DIENSTVEREINBARUNG FÜR LEHRER UND LEHRERINNEN

Bevor Office 365 Education als Plattform genutzt werden kann, sollten alle relevanten Entscheidungsträger in die Entscheidungsfindung eingebunden werden. Dazu können folgende Personengruppen gehören:

- Schulleitung
- Lehrervertretung bzw. Personalrat in der Schule oder beim Schulamt
- Schüler- und Elternvertretung

Um möglichst alle Beteiligten rechtzeitig einzubinden, ist es empfehlenswert, auch folgende Personen hinzuzuziehen.

- Datenschutzbeauftragter der Schule
- Systembetreuer der Schule (auch Externe, wie z.B. ein Systemhaus oder IT-Partner)
- Schulträger (Stadt oder Landkreis), wichtig für die Finanzierung

Bei den schulinternen Entscheidern (Schulleitung, Datenschutzbeauftragter, Systembetreuer, Schüler-/Elternvertretung) reicht meist eine Schulkonferenz aus, um einen Entschluss zu fassen.

Ein Muster für einen „Beschluss der Schulkonferenz“ und eine Dienstvereinbarung zwischen Schule und Personalrat liegen dem Anhang bei.

### 3.2.3. EINWILLIGUNG DER NUTZER

Wenn eine Schule für einen engen Benutzerkreis Office 365 testweise einsetzen möchte, können Sie von diesen Benutzern eine Einwilligungserklärung als datenschutzrechtliche Grundlage unterzeichnen lassen (Art. 6 Abs. 1 lit. a DSGVO). Beachten Sie, dass Sie aufgrund der Freiwilligkeit keine damit zusammenhängenden verpflichtenden Aufgaben oder Schülerbewertungen veranlassen sollten. Eine Muster-Einwilligung ist im Anhang zu finden.

## 3.3. DATENSCHUTZBEAUFTRAGTER

Als Bildungseinrichtung ist gemäß Art. 37 Abs. 1 DSGVO ein Datenschutzbeauftragter zu benennen. Zu den Aufgaben eines Datenschutzbeauftragten an einer Schule gehören:



- Beratung der Schulleitung, Kollegen und Schüler
- Hinwirken auf die Einhaltung rechtlicher Vorschriften
- Ansprechpartner für Betroffene (intern/extern)
- Ansprechpartner für die Aufsichtsbehörde

Für die Tätigkeit des DSB und für die Datenschutzdokumentation können beigefügte Muster genutzt werden.

### 3.4. AUFTRAGSVERARBEITUNG

Wenn Office 365 Education als Plattform zum Einsatz kommt, tritt Microsoft hier als Auftragsverarbeiter gemäß Art. 28 DSGVO auf. Der entsprechende Auftragsverarbeitungsvertrag heißt *Microsoft Online Services Terms*\* und wurde im Januar 2020 durch den *Anhang zu den Datenschutzbestimmungen für Onlinedienste*\*\* ergänzt, der auch die Standardvertragsklauseln als Vertragsbestandteil enthält und mit der EU-Datenschutzbehörde abgestimmt wurde.

Des Weiteren ist wichtig, dass Microsoft für den Betrieb weitere Unterauftragsverarbeiter in Anspruch nimmt. Eine Liste dieser liegt hier vor (<https://aka.ms/uav>).

\*) <http://www.microsoftvolumelicensing.com/Downloader.aspx?documenttype=OST&lang=German>

\*\*) <https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=16042>

### 3.5. VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN UND TECHNISCHE/ORGANISATORISCHE MAßNAHMEN

Die Online-Lernplattform ist so zu konfigurieren, dass ausschließlich die zur pädagogischen Aufgabenerfüllung der Schule erforderlichen Daten erhoben und verarbeitet werden.

Bei der Benutzerverwaltung durch den Administrator ist zwischen dem Anzeigenamen und dem Anmeldenamen zu unterscheiden. Der Anzeigename kann den Klarnamen (Vor-/Nachname) des Benutzers enthalten. Der Klarnamen ist zur Identifikation des Schülers durch Lehrer und Schüler erforderlich und muss nicht dem Anmeldenamen entsprechen. Der Anmelde-name (Teil der Email-Adresse) wird bei der Anmeldung im System verwendet und muss nicht mit dem Benutzernamen identisch sein. Die Nutzung von Pseudonymen als Anmeldenamen kann die Sicherheit im Vergleich zur Nutzung des Klarnamens erhöhen, erhöht aber auch die Komplexität der Nutzung.

Zumindest für die Lehrer und Verwaltung der Schule empfehlen wir, die in Office 365 integrierte und komfortable Möglichkeit der Zwei-Faktor-Anmeldung zu nutzen. Damit ist die Gefahr eines Identitätsdiebstahls stark vermindert. Office 365 bietet darüber hinaus eine sehr komfortable Möglichkeit, Daten und E-Mails zu verschlüsseln („Azure Information Protection“) und bietet einen wirksamen Schutz gegen komplexe Bedrohungen („Office 365 Advanced Threat Protection“).

Folgende Rollen sind in einer Online-Lernplattform in der Regel vorgegeben:

- Administrator: Der Administrator hat alle Berechtigungen für sämtliche Bereiche und Inhalte, er kann Benutzerkonten-Einstellungen ändern und systemweite Einstellungen vornehmen.
- Kursverwalter: Der Kursverwalter kann Bereiche anlegen und Berechtigungen vergeben. Das Recht kann auf Teilbereiche (Kurskategorien, beispielsweise Ausbildungsgänge, Fächer, Jahrgangsstufen) beschränkt werden.
- Lehrkraft: Die Lehrkraft kann in bestimmten Bereichen Inhalte pflegen, Teilnehmer zulassen, Lernfortschritte und Lernergebnisse einsehen.

- Teilnehmer: Teilnehmer können in den Bereichen arbeiten, zu denen sie eine Zugangsberechtigung haben, Lerninhalte nutzen und Eingaben tätigen.

In Übereinstimmung mit dem Rollen- und Berechtigungskonzept der Schule können weitere Rollen definiert werden.

Benutzerkonten von Schülern und Lehrern sind nach deren Ausscheiden aus der Schule zu löschen (bei einer pädagogischen Plattform gemäß Art. 6 Abs. 1 lit. c und e DSGVO) oder wenn diese ihre Einwilligung bei einem Piloten widerrufen (bei Einwilligung nach Art. 6 Abs. 1 lit. a DSGVO).

Ein Muster für technische und organisatorische Maßnahmen finden Sie im Anhang.

### 3.6. NUTZUNGSORDNUNG

Die Nutzungsordnung als Ergänzung zur gültigen Hausordnung der Schule gilt für die Benutzung der schulischen IT-Systeme und Computer (inklusive Tablets) an der Schule innerhalb und außerhalb des Unterrichts. Sie trägt dazu bei, ein höheres Maß an Datenschutz und einen optimalen Zustand dieser Einrichtungen zu gewährleisten. Dies ist Voraussetzung dafür, dass jederzeit effektiv mit den neuen Medien gearbeitet werden kann.

Ein mögliches Muster für eine Nutzungsordnung die Office 365 inkludiert liegt dem Anhang bei.

### 3.7. ZUSAMMENFASSUNG

Um Office 365 Education in einer Bildungseinrichtung nutzen zu können müssen die durch die DSGVO geforderten Schritte eingehalten und dokumentiert werden. Die wichtigsten Punkte die dabei zu beachten sind:

- Positive **Prüfung** des Anbieters anhand offizieller **Zertifizierung** des Cloud-Anbieters gemäß Art. 42 DSGVO (ISO 27001, ISO 27018, BSI C5, Privacy Shield, etc.)
- Vorliegen eines **Auftragsverarbeitungsvertrag** gemäß Art. 28 DSGVO (AVV)
- Vorliegen einer **Rechtsgrundlage** gemäß Art. 6 DSGVO
  - Vorliegen einer **Verpflichtung** gemäß Art. 6 Abs. 1 lit. c und e, Abs. 2 und 3 DSGVO im Verbund mit dem entsprechenden Absatz des Schulgesetzes und
    - **Beschluss** der Schulkonferenz (Schulleitung und Berater, Personalrat/Schülerbeirat/Elternbeirat)
  - oder Vorliegen einer **Einwilligung** gemäß Art. 6 Abs. 1 lit. a iVm Art. 7 DSGVO
- Vorliegen eines **Verzeichnisses von Verarbeitungstätigkeiten** gemäß Art. 30 DSGVO (VVV)
- Vorliegen **technischer und organisatorischer Maßnahmen** gemäß Art. 25, 32 DSGVO (TOM)
- Vorliegen einer schulspezifischen **Nutzungsordnung**

Folgend sind die wichtigsten Schritte in einer Übersicht zusammengefasst.

3.7.1. Wichtig bei der Einführung ist, möglichst früh alle Beteiligten an den Tisch zu holen und offen über die Bedenken und nächsten konkreten Schritte sprechen. Als ersten Schritt sollte es über die Schulkonferenz (Schulforum, Schulvorstand oder Schulausschuss) eine Entscheidung über die Nutzung von Office 365 herbeigeführt werden.

3.7.2. Aus diesem Entschluss leitet sich die notwendige Rechtsgrundlage ab. Dabei lässt sich die Rechtsgrundlage in vier Hauptszenarien einteilen:

1. **Office 365 soll nur für Lehrkräfte eingeführt werden.**  
Als rechtliche Grundlage kann dann Art. 6 Abs.1 lit c und e DSGVO genutzt werden. Ein Muster für den erforderlichen Eintrag in das Verzeichnis der Verarbeitungstätigkeiten liegt dem Anhang bei. Da es sich bei Office 365 um eine technische Einrichtung handelt, die zur Leistungs- und Verhaltenskontrolle geeignet ist, unterliegt die Einführung der Mitbestimmung durch den Personalrat, insofern dieser vorhanden ist. Eine Muster-Dienstvereinbarung zur Einführung von Office 365 liegt ebenfalls dem Anhang bei.
2. **Office 365 soll für Lehrkräfte und Schüler eingeführt werden, durch das Schulgesetz ihres Bundeslandes ist Nutzung einer Lern-/Lehrplattform geregelt.**  
In diesem Fall wäre als rechtliche Grundlage der Art. 6 Abs.1 lit e DSGVO in Verbindung mit dem entsprechenden Paragraphen aus dem Schulgesetz anzuführen. Die Beteiligungsrechte des Personalrates werden hierdurch nicht berührt. Die obige Muster-Dienstvereinbarung kann auch hier als Vorlage dienen.
3. **Office 365 soll für Lehrkräfte und Schüler eingeführt werden, im Schulgesetz ihres Bundeslandes ist der Einsatz einer Lernplattform o.ä. nicht verankert.**  
Demzufolge können Sie wie unter Punkt 1 beschrieben verfahren.
4. **Office soll 365 zuerst in einem Testbetrieb erprobt werden,** so ist am sinnvollsten mit der Einwilligung der Beteiligten zu arbeiten. Eine Muster-Einwilligung liegt dem Anhang bei. Wenn Schüler an diesem Pilotbetrieb beteiligt sind, so ist deren Einwilligung nur möglich, wenn sie 16 Jahre oder älter sind. Ansonsten ist eine Einwilligung der Erziehungsberechtigten einzuholen.

3.7.3. Ein gesonderter Auftragsverarbeitungsvertrag mit Microsoft muss nicht geschlossen werden. Dieser ist Bestandteil der *Microsoft Online Services Terms* (<http://www.microsoftvolume licensing.com/Downloader.aspx?documenttype=OST&lang=German>) zusammen mit dem *Anhang zu den Datenschutzbestimmungen für Onlinedienste* (<https://aka.ms/dpa>), der bei Abschluss eines Rahmenvertrags oder bei Lizenzkauf gilt.

3.7.4. Nun beginnt die Schreiarbeit. In den VVVs und TOMs müssen alle benötigten Informationen dokumentiert werden. Auch wenn dies viel Arbeit ist, so ist es notwendige Arbeit. Ein schöner Nebeneffekt ist, dass sich durch die Datenschutz- Dokumentation die technischen und organisatorischen Maßnahmen leichter ableiten und einführen lassen. Entsprechende Muster sind im Anhang zu finden.

3.7.5. Diese Maßnahmen können dann ebenfalls für die Nutzungsordnung und Datenschutzerklärung genutzt werden. Auch hier sind Muster-Vorlagen im Anhang beigelegt.

3.7.6. Zum Schluss gilt es dann die entsprechenden Dokumente zu sammeln und in einer ordentlichen Dokumentation zusammenzufassen. Eine Übersicht über die wichtigsten Dokumente von Microsoft (darunter die Datenschutzerklärung und die OST) sind in der Linksammlung im Anhang zu finden.

## 4. ANHANG

### 4.1. ABKÜRZUNGEN

Abs.	Absatz
Art.	Artikel
AV	Auftragsverarbeiter
AVV	Auftragsverarbeitungsvertrag
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
DSB	Datenschutzbeauftragter
DSGVO	Europäische Datenschutzgrundverordnung
iVm	In Verbindung mit
KM	Kultusministerium
LDSB	Landesdatenschutzbeauftragter
lit.	littera
MFA	Multi-Faktor-Authentifizierung
O365	Office 365
OST	Online Service Terms
TOM	Technische und Organisatorische Maßnahmen
UAV	Unterauftragsverarbeiter
VVV	Verzeichnis von Verarbeitungstätigkeiten
z.B.	Zum Beispiel

### 4.2. LINKS/QUELLEN/NORMEN

Name der Seite	Link	aka.ms Link
CELA Cloud-Kompendium	<a href="https://www.drvis.de/docs/Cloud%20Compendium%20March%202019_DE.pdf">https://www.drvis.de/docs/Cloud%20Compendium%20March%202019_DE.pdf</a>	<a href="https://aka.ms/cela-cloud-kompendium">https://aka.ms/cela-cloud-kompendium</a>
Datenschutz-konferenz veröffentlicht Kurzpapiere zum neuen Datenschutzrecht	<a href="https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html">https://www.bfdi.bund.de/DE/Home/Kurzmeldungen/DSGVO_Kurzpapiere1-3.html</a>	<a href="https://aka.ms/kurzpapiere">https://aka.ms/kurzpapiere</a>
GDD Praxishilfe XII	<a href="https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_12.pdf">https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_12.pdf</a>	<a href="https://aka.ms/gdd-praxishilfe">https://aka.ms/gdd-praxishilfe</a>
Leitfaden für die datenschutzkonforme Auswahl und den Betrieb von Lern-, Informations- und Kommunikationsplattformen an Schulen	<a href="https://it.kultus-bw.de/Lde/Startseite/IT-Sicherheit/Elektronische+Lernen+Informations+und+Kommunikationsplattformen">https://it.kultus-bw.de/Lde/Startseite/IT-Sicherheit/Elektronische+Lernen+Informations+und+Kommunikationsplattformen</a>	<a href="https://aka.ms/leitfaden-plattformen">https://aka.ms/leitfaden-plattformen</a>
Link zu Microsoft Online Services Terms	<a href="http://www.microsoftvolume licensing.com/Downloader.aspx?documenttype=OST&amp;lang=German">http://www.microsoftvolume licensing.com/Downloader.aspx?documenttype=OST&amp;lang=German</a>	<a href="https://aka.ms/ost_new">https://aka.ms/ost_new</a>

Link zu Anhang zu den Datenschutzbestimmungen für Onlinedienste	<a href="https://www.microsoftvolumeicensing.com/Downloader.aspx?DocumentId=16042">https://www.microsoftvolumeicensing.com/Downloader.aspx?DocumentId=16042</a>	<a href="https://aka.ms/dpa">https://aka.ms/dpa</a>
MFA Setup Hilfe (Mehrfaktoranmeldung)	<a href="https://aka.ms/mfasetup">https://aka.ms/mfasetup</a>	<a href="https://aka.ms/mfasetup">https://aka.ms/mfasetup</a>
O365 Roadmap	<a href="https://www.microsoft.com/de-de/microsoft-365/roadmap?filters=">https://www.microsoft.com/de-de/microsoft-365/roadmap?filters=</a>	<a href="https://aka.ms/o365-roadmap_new">https://aka.ms/o365-roadmap_new</a>
O365 Services	<a href="https://technet.microsoft.com/de-de/library/office-365-service-descriptions.aspx">https://technet.microsoft.com/de-de/library/office-365-service-descriptions.aspx</a> (-> <a href="http://aka.ms/Wkcowi">http://aka.ms/Wkcowi</a> )	<a href="https://aka.ms/o365-services">https://aka.ms/o365-services</a>
O365 Userprofil	<a href="https://portal.office.com/account/#personalinfo">https://portal.office.com/account/#personalinfo</a>	<a href="https://aka.ms/o365-userprofil">https://aka.ms/o365-userprofil</a>
Orientierungshilfe der Datenschutzaufsichtsbehörden für Online-Lernplattformen im Schulunterricht	<a href="https://www.datenschutzkonferenz-online.de/media/oh/20180426_oh_online_lernplattformen.pdf">https://www.datenschutzkonferenz-online.de/media/oh/20180426_oh_online_lernplattformen.pdf</a>	<a href="https://aka.ms/orientierungshilfe">https://aka.ms/orientierungshilfe</a>
Standard-Datenschutzmodell	<a href="https://www.bfdi.bund.de/DE/Datenschutz/Themen/TechnischeAnwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html">https://www.bfdi.bund.de/DE/Datenschutz/Themen/TechnischeAnwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html</a>	<a href="https://aka.ms/datensicherheitsmodell">https://aka.ms/datensicherheitsmodell</a>
Trustcenter	<a href="http://www.trustcenter.office365.de">http://www.trustcenter.office365.de</a>	<a href="https://aka.ms/trustcenter_new">https://aka.ms/trustcenter_new</a>
UAV	<a href="https://www.microsoft.com/de-de/trust-center/privacy/data-access">https://www.microsoft.com/de-de/trust-center/privacy/data-access</a>	<a href="https://aka.ms/uav">https://aka.ms/uav</a>
Unterauftragnehmer	<a href="https://www.microsoft.com/de-de/trustcenter/privacy/data-management/data-access">https://www.microsoft.com/de-de/trustcenter/privacy/data-management/data-access</a>	<a href="https://aka.ms/unterauftragnehmer">https://aka.ms/unterauftragnehmer</a>
IT-Grundschutz-Kataloge	<a href="https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html">https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html</a>	<a href="https://aka.ms/kataloge">https://aka.ms/kataloge</a>
Strategie der Kultusministerkonferenz „Bildung in der digitalen Welt“	<a href="https://www.kmk.org/themen/bildung-in-der-digitalen-welt/strategie-bildung-in-der-digitalen-welt.html">https://www.kmk.org/themen/bildung-in-der-digitalen-welt/strategie-bildung-in-der-digitalen-welt.html</a>	<a href="https://aka.ms/strategie-kultusministerkonferenz">https://aka.ms/strategie-kultusministerkonferenz</a>

Schulgesetze der Länder in der Bundesrepublik Deutschland	<a href="https://www.kmk.org/dokumentation-statistik/rechtsvorschriften-lehrplaene/uebersicht-schulgesetze.html">https://www.kmk.org/dokumentation-statistik/rechtsvorschriften-lehrplaene/uebersicht-schulgesetze.html</a>	<a href="https://aka.ms/schulgesetze-laenderebene">https://aka.ms/schulgesetze-laenderebene</a>
Europäische Datenschutzgrundverordnung	<a href="https://dsgvo-gesetz.de/">https://dsgvo-gesetz.de/</a>	<a href="https://aka.ms/dsgvo-grundverordnung">https://aka.ms/dsgvo-grundverordnung</a>
Microsoft Complianceangebote	<a href="https://www.microsoft.com/de-de/trustcenter/compliance/complianceofferings">https://www.microsoft.com/de-de/trustcenter/compliance/complianceofferings</a>	<a href="https://aka.ms/compliance-angebote">https://aka.ms/compliance-angebote</a>

## 4.3. MUSTER

A1\_Checkliste für Kurzaudits

A2\_VerarbeitungsverzeichnisVerantwortlicher\_Schulen

A3\_Muster\_Beschluss\_Schule

A4\_Muster-Dienstvereinbarung-Schule

A5\_Nutzungsordnung-Schule (2 Varianten)

A6\_Einwilligung -Schule (2 Varianten)

A7\_Technische und Organisatorische Maßnahmen für Verantwortliche

A8\_Umgang mit Eltern

Grace-Hopper-Gesamtschule

AI

Checkliste für Kurzaudits



**Kurzübersicht Audit Dokumente:**

<b>Unterlagen Organisation</b>	<b>Vorhanden?</b>
Verzeichnis der Verarbeitungstätigkeiten (DSGVO)	
Technische und Organisatorische Maßnahmen (DSGVO)	
Datenschutzerklärung	
<b>Unterlagen zum Datenschutzbeauftragten</b>	
Bestellungsurkunde	
Nachweis der Fähigkeiten	
Nachweis der Fortbildungen	
Schulungsunterlagen für die Datenschutz-Mitarbeiter	
Dokumentation IT (Infrastruktur, Backup, Firewall, Virenschutz, etc.)	
Berechtigungskonzepte (Server/Dateisysteme, Datenbanken, etc.)	
<b>Dienstvereinbarung</b>	
Private Internet-/E-Mail-/Gerätenutzung	
Arbeitsplätze im Rahmen des „Home-Offices“	
<b>Sonstige datenschutzrelevante Vereinbarungen</b>	
Dokumentenmanagementsystem	
Nutzungsordnung der Schule	
<b>Vereinbarungen zur Nutzung</b>	
physischer/virtueller PC	
Laptop	
Tablet	
Handy/Smartphone	
RAS-/VPN-Zugänge	

<b>Arbeitsanweisungen</b>	
Nutzung Administratoraccount	
Backup	
Nutzung/Verwendung/Vernichtung/Transport/Archivierung externer Datenträger	
Besucherregelung	
Nutzung Aktenvernichter	
Vorgehen bei Verlust Schlüssel	
Datenträgertransport/-vernichtung/-nutzung/-aufbewahrung	
<b>Liste der Auftragsverarbeiter</b>	
IT-Outsourcing	
Wartung für IT und Telekommunikation	
Subunternehmer	

Grace-Hopper-Gesamtschule

A2

Verarbeitungsverzeichnis für Verantwortliche an Schulen

# Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen gem. Artikel 30 Abs. 1 DSGVO

## 1. Allgemeine Angaben

Bezeichnung der Verarbeitungstätigkeit	Office365 – Exchange Online, SharePoint Online, Teams, Installation der Desktopanwendungen
Verantwortlicher gem. Artikel 30 Abs. 1 DSGVO (Bezeichnung der Schule, Anschrift, E-Mail-Adresse und Telefonnummer)	Grace-Hopper-Gesamtschule, Albert-Wiebach-Str. 4, 14513 Teltow
Falls zutreffend: Angaben zu weiteren gemeinsam für die Verarbeitung Verantwortlichen (jeweils Bezeichnung, Anschrift, E-Mail-Adresse und Telefonnummer)	/
Datum der Einführung	01.08.2020
Stand dieser Dokumentation	30.08.2020
Behördlicher Datenschutzbeauftragter (Name, dienstliche Anschrift, E-Mail-Adresse, Telefonnummer)	Torsten Leis Magdeburger Str. 45, 14470 Brandenburg an der Havel, Torsten.Leis@schulaemter.brandenburg.de, 03381-39-7425

## 2. Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)

Zweck	<ul style="list-style-type: none"> <li>IT-gestützte Zusammenarbeit der Mitarbeiter und Schüler der Schule mittels der Microsoft Office 365 Dienste Exchange Online, Sharepoint Online und der Lernplattform Teams.</li> <li>Unterstützung von Schulen bei der Erfüllung ihrer durch Rechtsvorschriften zugewiesenen Aufgaben mit Hilfe von Microsoft Office365 zur Umsetzung des Bildungs- und Erziehungsauftrags, bei der Abwicklung der schulinternen Aufgaben und Abläufe und der Umsetzung der Medienkompetenzen im Rahmen der Digitalisierung.</li> </ul> <p>Besonders sind dies:</p> <ul style="list-style-type: none"> <li>- E-Mailkommunikation mit Termin- und Ressourcenverwaltung, gemeinsame Kalender, Office 365 Gruppen</li> <li>- Bereitstellung und Austausch von Dokumenten</li> <li>- Projektverwaltung zur Organisation der schulischen Abläufe, Chatfunktion</li> <li>- Lernplattform Teams mit Klassennotizbüchern, Bereitstellung von Unterrichtsmaterialien, Aufgaben mit Terminabgabe, Bewertung, Rückmeldung</li> <li>- Nutzung der Desktopversion von Office</li> </ul>
Name des eingesetzten Verfahrens	Microsoft Office 365 ( <a href="http://aka.ms/Wkcowi">http://aka.ms/Wkcowi</a> )
Dienstbeschreibungen	<a href="https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx">https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx</a> und <a href="https://technet.microsoft.com/en-us/library/office-365-service-descriptions.aspx">https://technet.microsoft.com/en-us/library/office-365-service-descriptions.aspx</a>

### 3. Rechtsgrundlagen:

- Bestimmungen der Schulordnungen, des Schulgesetzes und der Lehrerdienstordnung
- Art. 6 Abs. 1 S. 1 lit c und e DSGVO
- Art. 6 und 9 DSGVO
- Zuständige Aufsichtsbehörde

### 4. Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)

- Lehrkräfte, nicht unterrichtendes Personal, Verwaltungspersonal der Schule sowie externes Betreuungspersonal, das an der Schule tätig ist
- Alle Schüler, die im laufenden Schuljahr die Schule besuchen oder besucht haben

### 5. Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)

Daten zu Lehrkräften und zum nicht unterrichtenden Personal	<ul style="list-style-type: none"><li>• Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, E-Mailadresse, weitere dienstliche E-Mailadressen, Funktion, dienstliche Telefonnummer falls bestehend)</li><li>• Gruppenzugehörigkeiten in Teams, Mitbesitzer eines Teams, unterrichtete Fächer, unterrichtete Klassen</li></ul>
Daten der Schüler	<ul style="list-style-type: none"><li>• Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, Funktion)</li><li>• Schulart, Klasse, Jahrgangsstufe</li><li>• Besuchte Unterrichtseinheiten, für die Teams eingerichtet werden</li><li>• Unterrichtselemente (Lehrstoff, Leistungserhebungen, Aufgabenzuteilungen, Bewertungen)</li></ul>
Daten aller Nutzer	<ul style="list-style-type: none"><li>• Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, Funktion)</li><li>• Berechtigungen</li><li>• Log-Daten (Datum der letzten Passwortänderung, Datum der letzten Anmeldung, Größe und Zahl der gespeicherten Daten)</li><li>• Historisierung (Information über angelegte/geänderte/gelöschte Datensätze)</li></ul>
Vom den Nutzern erzeugte Inhalte und Einstellungen	<ul style="list-style-type: none"><li>• persönliche Einstellungen, Angaben in Nutzerprofil, gespeicherte Inhalte in E-Mail, Chats, Kalendereinträge, Kommentare, Datenbankeinträge, Daten der unterrichteten bzw. verwalteten Schüler</li><li>• Weitere Faktoren zur Anmeldung mittels Multi-Faktor-Authentifizierung (Telefon oder private E-Mail oder App oder Fragen)</li></ul>
Besondere Kategorien personenbezogener Daten (Art. 9)	keine

**6. Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)**

	<b>Empfänger</b>	<b>Zweck</b>	<b>Daten</b>
<b>Intern</b>	Mitarbeiter und Schüler	Zusammenarbeit und IT-gestützter Unterricht	eingeschränkte Lese- und/oder Schreibrechte in den Teams und Office 365 Gruppen, deren Mitglied sie sind und in den Dokumentenbibliotheken und öffentlichen Kalendern, die ihnen freigegeben wurden
	Systembetreuer	Konfiguration, Überwachung und Sicherung des Betriebs, Support	administrative Lese-, Schreib- und Löschrechte entsprechend den ihnen zugeteilten Rechten auf alle oder bestimmte Office 365 Dienste
<b>Extern</b>	Alle Empfänger von E-Mails	Kommunikation	Anzeigenname, E-Mailadresse
	Ireland Operations Limited, Carmanhall Road, Sandyford Industrial Estate, Dublin 18, Irland	Dienstbereitstellung, Service und Support	<ul style="list-style-type: none"> <li>• von den Benutzern gespeicherte Daten: Die Speicherung erfolgt nur innerhalb der EU in nach ISO 27001, 27002, ISO/IEC 27018 zertifizierten Rechenzentren im Rahmen des AV Vertrags <a href="http://aka.ms/Wkcowi">http://aka.ms/Wkcowi</a>, der die EU Standardvertragsklauseln enthält.</li> <li>• Anmeldedaten: Speicherung in allen Microsoft-Anmeldeservern</li> </ul>

**7. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)**

- Microsoft Ireland beschäftigt Unterauftragsnehmer in Drittländern, insbesondere Microsoft Corporation in USA, die sich den EU Standardvertragsklauseln unterworfen haben. Diese Unterauftragsnehmer sind unter folgendem Link vollständig aufgeführt: <https://www.microsoft.com/de-de/trustcenter/privacy/data-management/data-access>.
- Wenn ein neuer Dienst in Office 365 angeboten wird, werden die damit verbundenen Daten in USA verarbeitet. Diese Dienste werden vom Systembetreuer ausgeschaltet.

**8. Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)**

Verlässt ein Mitarbeiter die Schule, wird sein persönliches Office 365 Konto inklusive aller gespeicherten Daten nach 3 Monaten gelöscht. Die Rechte auf weitere Office 365 Konten werden ihm gleichzeitig entzogen.

**9. Technische und organisatorische Maßnahmen gemäß Art. 32 Abs. 1 DSGVO**

Die technisch-organisatorischen Maßnahmen in den EU Rechenzentren von Microsoft Irland sind durch die Zertifizierung und die Angaben in diesem Link <http://www.trustcenter.office365.de> aufgeführt. Die verbleibenden Maßnahmen, die hier beschrieben wird, sind die Maßnahmen zur Sicherung des Internet-Zugangs zu den Microsoft Diensten in Office 365 und zur sicheren Speicherung von Zugangsdaten auf den Clients des Verantwortlichen.

Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)	Zutrittskontrolle	die Anmeldung an Office 365 erfolgt im Browser per verschlüsseltem und eingeschränktem Authentifizierungsverfahren nach dem OAuth2 Protokoll. Die Büroraume sind nur berechtigten Personen zugänglich und außerhalb der Dienstzeiten gesperrt.
	Zugangskontrolle	Das Schulnetzwerk ist durch eine Firewall geschützt. Die E-Mail in Office 365 ist durch die Sichere-Links- und Sichere-Anhangs-Technologie geschützt. Die Desktop Betriebssysteme der Verwaltungsmitarbeiter und Systembetreuer sind Windows 10 Enterprise und durch Applikations- und Makro- Kontrolle geschützt.
	Zugriffskontrolle	Die Benutzerkonten der Verwaltungsmitarbeiter und Systembetreuer sind durch Multi-Faktor-Anmeldung oder biometrische Anmeldung gesichert.
	Trennungskontrolle	Administrativer Zugriff auf die Office 365 Instanz der Schule ist auf die vom Schulleiter bestellten Systembetreuer beschränkt.
Integrität (Art. 32 Abs. 1 lit. b DS-GVO)	Weitergabekontrolle	Im Rahmen der Nutzung von Microsoft Online Diensten liegt die Umsetzung der Weitergabekontrolle bei Microsoft. Microsoft setzt im Rahmen der Online Dienste bei der Datenübertragung über das Internet auf TLS Verschlüsselung (https Protokoll).
	Eingabekontrolle	Die Konsistenz und Gültigkeit der Benutzerkonten in den Office 365 Instanzen ist durch die tägliche Anmeldung der Benutzer, die Sichtbarkeit der Benutzerkonten in den Adresslisten und Verzeichnissen gewährleistet.
Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)	Verfügbarkeitskontrolle	Alle Benutzer-Anmeldedaten und Nutzerdaten liegen in den Microsoft EU Rechenzentren (die für deutsche Kunden in Frankfurt und Berlin liegen) und sind durch die spezifischen Sicherheitsmaßnahmen von Microsoft geschützt, insbesondere durch die Backup-Strategien von Microsoft (Datei-Versionierung, Spiegelung der virtuellen Instanzen).
	Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);	Dies ist serverseitig durch die mehrfache Spiegelung der virtuellen Instanzen in den Office 365 Instanzen gesichert (Microsoft Servicevertrag), Nutzerdaten in Office 365

		können vom Nutzer selbst mit einem Klick auf den Stand eines früheren Zeitpunkts wiederhergestellt werden.
Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)	Datenschutz-Management	Die regelmäßige Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung wird durch die Zertifizierung des Auftragnehmers gemäß Art. 42 DS-GVO gesichert.
	Incident-Response-Management	Falls ein illegitimer Zugriff auf eine Office 365 Instanz erfolgt, sind 2 Szenarien möglich: es werden zusätzliche Konten erstellt oder es werden Konten gelöscht. Gelöschte Konten und damit zusammenhängende Daten und E-mails können in Office 365 teils durch den Nutzer selbst, und teils durch einen speziellen Papierkorb, auf den nur der Administrator Zugriff hat, wiederhergestellt werden. Zusätzliche Konten erscheinen in den Adressbüchern und können kurzfristig gelöscht werden.
	Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO);	Die Mitarbeiter werden von den Systembetreuern auf die Möglichkeiten der Pseudonymisierung und sparsamen Speicherung personenbezogener Daten in Office 365 hingewiesen und dabei unterstützt.
	Auftragskontrolle	Die Office 365 Instanz gehört dem Auftraggeber, der alleine Zugriff auf die Nutzdaten hat.



Grace-Hopper-Gesamtschule

A3

Muster Beschluss Schule

## **Beschluss zum Einsatz der Lernplattform Office 365 an unserer Schule**

Die Schulkonferenz als oberstes Mitwirkungs- bzw. Beschlussgremium an unserer Schule, in dem die Schulleitung, die Vertretung der Lehrer, Eltern und Schüler vertreten sind, fasst am 15.09.2020 in Übereinstimmung mit Bestimmungen der Schulordnungen und Lehrerdienstordnung, sowie Art. 6 Abs. 1 S. 1 lit c und e der Datenschutzgrundverordnung den im Folgenden ausgeführten Beschluss.

**Vorbemerkung:** Wenn im Text aus Gründen der Lesbarkeit die männliche Form gewählt wird, gelten die Aussagen in gleicher Weise für Angehörige aller Geschlechter.

### **Gegenstand dieser Vereinbarung**

Diese Vereinbarung dient der Unterstützung unserer Schule bei der Erfüllung ihrer durch Rechtsvorschriften zugewiesenen Aufgaben mit Hilfe von Microsoft Office365 zur Umsetzung des Bildungs- und Erziehungsauftrags, bei der Abwicklung der schulinternen Aufgaben und Abläufe und der Umsetzung der Medienkompetenzen im Rahmen der Digitalisierung.

Unsere Schule ist verpflichtet, unseren Schülern eine zeitgemäße Medienkompetenz zu vermitteln, die Schüler mit den vielfältigen Einsatzmöglichkeiten moderner Medien vertraut macht und Ihnen die Chancen und Risiken dieser neuen Technologien in ausgewogener Form nahebringt.

Voraussetzung ist selbstverständlich, dass auch unsere Lehrerschaft mit denselben Technologien vertraut ist bzw. vertraut gemacht wird.

Eine grundlegende Anforderung dabei ist, dass die Schule die volle Kontrolle über Umfang, Art der Wissens-Vermittlung und Nutzung der Daten beim Einsatz von digitalen Lernplattformen behält. Es ist immer der Lehrer, der in jedem Fach und jeder Klasse in Absprache mit Schülern und Eltern entscheidet, in welcher Form Informationstechnologien den Unterricht sinnvoll ergänzen und bereichern können.

### **Konkretisierung dieser Vereinbarung**

Wir schlagen nach sorgfältiger Analyse der Angebote am Markt vor, die Lernplattform Microsoft Office 365 als eine der digitalen Angebote in unserer Schule einzusetzen. Diese Vereinbarung ergänzt den bereits bestehenden Einsatz der bisherigen Lernplattformen und internetgestützten schulischen Angebote.

### **Name des eingesetzten Verfahrens und Dienstbeschreibungen**

Microsoft Office 365 (<http://aka.ms/Wkcowi>)

<https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx>

<https://technet.microsoft.com/de-de/library/office-365-service-descriptions.aspx>)

### **Ort der Speicherung**

- Es ist vertraglich gesichert, dass alle Nutzdaten nur innerhalb der EU in den Rechenzentren von Microsoft (für deutsche Kunden liegen diese in Frankfurt und Berlin) gespeichert werden und von Microsoft in keiner Weise ausgewertet oder gelesen werden können.
- Alle Daten werden verschlüsselt über das Internet übertragen und in den Rechenzentren von Microsoft maschinell verschlüsselt gespeichert. Zugriff auf die Nutzdaten hat nur die Schule und die von der Schule beauftragten Systembetreuer.

## **Art der gespeicherten Daten**

Grundsätzlich sind die vorgegebenen Kontodaten in Office 365 keine besonders schutzwürdigen Daten, sondern nur solche, deren Verfügbarkeit innerhalb der Schule von den Betroffenen erwartet wird und das Minimum an Daten darstellt, das für die Erfüllung der Aufgaben des Einzelnen erforderlich ist.

- Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, E-Mailadresse, weitere dienstliche E-Mailadressen, Funktion, u. U. dienstliche Telefonnummer)
- Gruppenzugehörigkeiten in Teams
- Unterrichtsmaterial, Aufgaben

Weitere Detailangaben sind im Verfahrensverzeichnis des Verantwortlichen aufgeführt.

## **Beschreibung des Angebots**

Microsoft Office 365 bietet mit Microsoft Teams eine Lernplattform an. Dies ist ein intuitives, geräte- und orts-unabhängiges soziales Medium unter Kontrolle der Schule, das eine Whats-App ähnliche Kommunikation mit der Bereitstellung von Texten, Dokumenten, Bildern, Videos ermöglicht. Damit verknüpft ist ein modernes E-Mailsystem und Microsoft Office in der aktuellen Form, das lokal sowohl auf allen Schulgeräten, als auch auf den privaten Geräten der Schüler und Mitarbeiter installiert werden kann.

- Die Software steht auf allen üblichen Medien wie PCs, Macs, Tablets, Handys zur Verfügung und kann von all diesen Medien ortsunabhängig genutzt werden.
- Die Software steht für Schüler, Lehrer und Mitarbeiter einer Schule kostenlos zur Verfügung und kann jeweils gleichzeitig auf bis zu 10 Geräten installiert und genutzt werden.
- In Teams integriert sind E-Mail und Kalender, es können weitere Lernprogramme vom Lehrer in Teams integriert werden. Somit erhält jeder Schüler automatisch eine E-Mailadresse, über die dieser E-Mails empfangen und senden kann.
- Das System bietet die Möglichkeit, das Versenden von E-Mails auf die Mitglieder der Schule zu beschränken. Ebenso bietet das System die Möglichkeit, den Austausch von Dokumenten oder anderen Daten auf Mitglieder der Schule zu beschränken.
- Jeder Schüler hat einen eigenen Arbeitsbereich, der nur vom jeweils zuständigen Lehrer eingesehen werden kann, aber nicht von anderen Schülern. Lehrer können Dateien, Bilder und Videos bereitstellen, Aufgaben mit Abgabeterminen erstellen und diese Aufgaben bewerten. Schüler und Lehrer können untereinander und miteinander vertraulich Nachrichten austauschen.
- Grundsätzlich können sich die Systembetreuer Einsicht in alle gespeicherten Daten verschaffen und diese redigieren oder löschen, falls dies aus pädagogischen oder rechtlichen Gründen in Absprache mit den verantwortlichen Vertretern der Schulleitung, der Lehrer, der Eltern oder der Schülervertreter geboten ist.
- Für Lehrer und Mitarbeiter der Schule bietet Office 365 eine Ende-zu-Ende-Verschlüsselung der Daten und Mehrfaktoranmeldung an, um die Sicherheit der Daten nach Stand der Technik zu gewährleisten.

## **Datenschutzrechtliche Aspekte**

Der Einsatz einer digitalen Lernplattform schließt die automatisierte Verarbeitung personenbezogener Daten ein. Dies ist nach Artikel 6 1 c und e der DSGVO aufgrund unserer oben genannten Verpflichtung einer Schule rechtskonform.

Die Datenschutzverantwortung liegt bei unserer Schule. Wir legen im Anhang 1 fest, welche Daten gespeichert werden, wer darauf Zugriff hat, wer über die gespeicherten Daten Auskunft geben kann, welche Fristen für die Löschung der Daten nach Verlassen der Schule gelten.

## **Verfügbarkeit**

Microsoft garantiert eine weltweite Verfügbarkeit der Office 365 Dienste mit 99,9 % Wahrscheinlichkeit. Alle in Office 365 (OneDrive) gespeicherten Daten können auf lokalen Geräten synchronisiert werden, sodass Sie auch ohne Internet verfügbar sind.

## **Sicherheit und Integrität der Daten und der Schutz vor Identitätsdiebstahl**

Office 365 ermöglicht eine Ende-zu-Ende Verschlüsselung aller E-Mails und Dokumente. Das Verfahren heißt Azure Information Protection und ermöglicht dem Lehrer, Dokumente auf einfache Weise so zu schützen, dass diese nur mehr von den voreingestellten Gruppen von Benutzern von Office 365 geöffnet und gelesen oder gelesen und geändert werden können. Diese Verschlüsselung ist zertifikatsbasiert.

Office 365 bietet standardmäßig eine komfortable Mehrfaktoranmeldung an, wobei der Benutzer selbst aus einer ganzen Reihe von Anmeldefaktoren wählen kann. Diese Anmeldedaten sind auch den Administratoren nicht zugänglich und können nur vom Benutzer selbst geändert werden.

## **Vertraulichkeit der Daten und Nichtverkettung**

Die Vertraulichkeit der in Office 365 gespeicherten Daten ist durch detaillierte Rechtezuweisungen garantiert. Standardmäßig sind vom Benutzer gespeicherte Daten nur für ihn selbst zugänglich und er muss diese explizit anderen Benutzern zum Lesen oder zum Lesen und Bearbeiten freigeben.

## **Schutz der Privatsphäre**

Auf allen modernen Geräten laufen Office 365 Apps wie Onedrive oder Teams oder Outlook am Web in einem Isolationsmodus, sodass andere Apps keinen Zugriff auf diese Daten erhalten.

## **Intervenierbarkeit und Widerspruch**

Jedes Mitglied der Schule hat das Recht, nicht nur Auskunft, sondern auch eine rasche Korrektur der personenbezogenen Daten zu verlangen, wenn diese nicht aktuell oder richtig sind. Außerdem kann jedes Mitglied der Speicherung weiterer personenbezogener Daten, die über das oben angegebene Minimum hinausgehen, jederzeit zu widersprechen. Dies ist formlos beim Datenschutzbeauftragten Herr Torsten Leis möglich.

## **Technische und organisatorische Maßnahmen**

Die technisch-organisatorischen Maßnahmen in den EU Rechenzentren von Microsoft Irland sind durch die Zertifizierung und die Angaben in diesem Link <http://www.trustcenter.office365.de> aufgeführt. Die verbleibenden Maßnahmen sind im Verfahrensverzeichnis des Verantwortlichen beschrieben.

## **Eingriff in Grundrechte**

Wie dargelegt, sind die personenbezogenen Daten in Office 365 sicher nach Stand der Technik und inkludieren nur die minimalen Daten, die für die Erledigung der schulischen Aufgaben erforderlich ist.

Der Eingriff in die Grundrechte und Grundfreiheiten der Benutzer wird durch die beschriebenen technischen und organisatorischen Maßnahmen wirksam auf ein minimales Risiko reduziert.

## **Prüfung durch Datenschutzbeauftragten**

Der Datenschutzbeauftragte unserer Schule Herr Torsten Leis hat das Angebot von Office 365 geprüft und die Erfüllung der datenschutzrechtlichen Anforderungen des Angebots in der beabsichtigten Einsatzform bestätigt, wenn auch als bedenklich klassifiziert.

## **Beschlusspunkte**

1. Umfang: Es besteht Einvernehmen, dass der Einsatz digitaler Medien nicht zu einer Mehrbelastung der Schüler führen darf. Eltern können sich bei dahingehenden Problemen oder Fragen an den Beratungslehrer Herr Andreas Fischer oder an den Schulleiter und seinen Stellvertreter persönlich, schriftlich, per E-Mail oder per Telefon melden.
2. Lehrer: der Einsatz und Umfang des Einsatzes von Office 365 in einem Fach, einer Klasse oder Unterrichtseinheit obliegt der freien Entscheidung des jeweiligen Lehrers.
3. Schüler: Schüler können Vorschläge, Probleme oder Fragen zu dem Einsatz der Lernplattform an die Schülervertreter, an ihren Klassenlehrer oder an den Beratungslehrer Herr Andreas Fischer persönlich melden.
4. es wird vereinbart, dass E-Mails auch mit Externen ausgetauscht werden können, das Teilen von Daten mit Externen aber eine Anmeldung an einen Microsoft Dienst oder einen per E-Mail zugestellten Code erfordert.
5. Dauer: diese Vereinbarung zum Einsatz von Office 365 als Lernplattform gilt ab Beschluss 1 Jahr und endet danach. Nach diesem Jahr evaluiert dieses Gremium diese Vereinbarung und kann danach eine Verlängerung beschließen. Die Regeln für die Gültigkeit des Beschlusses folgen aus der Satzung des Gremiums.

## **Anhang 1:**

Art der gespeicherten Daten: Vorname und Nachname des Schülers oder Lehrers, E-Mailadresse, Funktion des Benutzers, Unterrichtsmaterialien, Schüleraufgaben, von den Benutzern selbst freigegebene Daten. Die E-Mailadresse setzt sich aus Vor- und Nachnamen und der Schuldomäne zusammen.

Zugriff auf Daten: Zugriff auf die Daten haben unsere schulischen Systembetreuer Herr Maik Vogler und der von uns mit der Erst-Einrichtung der Office 365 Konten beauftragte Dienstleister Herr Maik Vogler mit dem ein gesonderter Auftragsverarbeitungsvertrag für diesen Zweck abgeschlossen wurde.

Auskunft über gespeicherte Daten: geben die schulischen Systembetreuer Herr Maik Vogler und der Datenschutzbeauftragte Herr Torsten Leis.

Löschfristen: Ein Office 365 Schülerkonto (bzw. Lehrerkonto) wird inklusive aller gespeicherten Daten 4 Wochen (bzw. 3 Monate) nach Verlassen der Schule irreversibel gelöscht.

Grace-Hopper-Gesamtschule

A4

Muster-Dienstvereinbarung-Schule

**Rahmen-Dienstvereinbarung**  
**zwischen**  
**Grace-Hopper-Gesamtschule, Albert-**  
**Wiebach-Straße 4, 14513 Teltow**  
**nachfolgend mit „Schule“ bezeichnet,**  
**und**  
**dem Lehrerrat der Grace-Hopper-**  
**Gesamtschule**  
**zum Einsatz vom Microsoft Office 365**

**§ 1 Präambel**

Zwischen Schule und PR besteht Einvernehmen darüber, dass die Schule zur Erfüllung ihrer dienstlichen Aufgaben eine moderne digitale Plattform benötigt, die eine fachgerechte Kommunikation und Zusammenarbeit unterstützt und ermöglicht. Ziel dieser Vereinbarung ist es, die Einbeziehung der Beschäftigten in die Nutzung von digitalen Plattformen sicherzustellen, die Mitbestimmungsrechte des Personalrats zu wahren und eine Beeinträchtigung der schutzwürdigen Belange von Beschäftigten zu verhindern.

**§ 2 Zielsetzung**

Ziel dieser Dienstvereinbarung (nachfolgend mit DV abgekürzt) ist es, die Zulässigkeit und Unzulässigkeit von Leistungs- und Verhaltenskontrolle speziell durch die technischen Möglichkeiten von Office 365 zu regeln. Die in dieser Dienstvereinbarung getroffenen Regelungen sind Ausdruck der Abwägung der Grundrechte der betroffenen Beschäftigten, insbesondere ihres Grundrechts der Menschenwürde, ihres Persönlichkeitsrechts sowie ihres Rechts auf informationelle Selbstbestimmung.

**§ 3 Gegenstand**

Diese Dienstvereinbarung regelt den Einsatz der Microsoft Office 365 Online Dienste. Die Nutzung der Dienste erfolgt ausschließlich zu dienstlichen Zwecken.

**§ 4 Geltungsbereich**

**§ 4.1. Räumlicher Geltungsbereich**

Der räumliche Geltungsbereich dieser Dienstvereinbarung erstreckt sich auf alle Einrichtungen und Gebäude der Schule.

**§ 4.2. Persönlicher Geltungsbereich**

Der persönliche Geltungsbereich erstreckt sich auf alle bei der Schule beschäftigten Arbeitnehmer.

**§ 5 Eingesetzte Office 365 Komponenten**

Die eingesetzten Komponenten von Office 365 und deren Konfiguration werden in den Anlagen A festgelegt. Dies sind ausschließlich die Bestandteile von Office 365, für die in den jeweils gültigen

„Bestimmungen für Onlinedienste“ der Microsoft Corporation die „Bestimmungen für die Datenverarbeitung“ und damit auch die EU-Standardvertragsklauseln gelten (derzeit z.B. Azure Active Directory, Exchange Online, SharePoint Online, Skype for Business, Teams, Yammer).



## **§ 6 Leistungs- und Verhaltenskontrolle**

Grundsätzlich dürfen weder Inhalts- noch Metadaten aus Office 365 zur Leistungs- und / oder Verhaltenskontrolle genutzt werden. Davon ausgenommen ist die unter § 8 ausgeführte Nutzung von Protokolldaten zur Sicherstellung der Betriebssicherheit. Arbeitsrechtliche Konsequenzen, die auf der Auswertung personenbezogener Daten aus Office 365 beruhen, sind generell unwirksam. Derartige Daten und Auswertungen unterliegen weiterhin einem Beweisverwertungsverbot. Hiervon abweichende Einzelfallregelungen zur Leistungs- und / oder Verhaltenskontrolle bedürfen der expliziten Zustimmung des PR und werden in separaten Dienstvereinbarungen dokumentiert.

## **§ 7 Durchführung der Mitbestimmung**

### **§ 7.1. Information / Abstimmung**

Um die Informations- und Mitbestimmungsrechte des PR wahrnehmen zu können, erhält der PR Zugriff auf das Office 365 Nachrichtencenter, in dem Microsoft alle anstehenden Änderungen und Updates für Office 365 rechtzeitig veröffentlicht. Zur weiteren Information steht außerdem die Microsoft 365 Roadmap unter <https://www.microsoft.com/de-de/microsoft-365/roadmap?filters=> zur Verfügung. Geplante Änderungen / Erweiterungen in Office 365, die den Einsatz in der Schule betreffen, werden zwischen der Schulleitung, den Systembetreuern und dem PR im Vorfeld abgestimmt.

### **§ 7.2. Erweiterung des Funktionsumfangs**

Der zur Nutzung freigegebene Funktionsumfang der eingesetzten Office 365 Komponenten kann durch Dokumentation der entsprechenden Komponenten in Anlage A erweitert werden. Die entsprechenden Anlagen sind dem PR unverzüglich, mindestens aber 2 Monate vor der geplanten Einführung der jeweiligen Funktion vorzulegen und mit diesem abzustimmen.

### **§ 7.3. Updates**

Reine Funktions- und Sicherheitsupdates, die keinen Einfluss auf mögliche Leistungs- und Verhaltenskontrolle haben, bedürfen keiner Dokumentation in der Anlage A.

### **§ 7.4. Rechte des Personalrats**

Der PR hat das Recht, jederzeit die Einhaltung dieser DV zu kontrollieren und dabei in alle Programme, Dateien und Auswertungen Einblick zu nehmen und von den Anwendern sowie Systemverantwortlichen Auskünfte einzuholen. Er kann auch jederzeit die Unterlagen zu den Systemkonfigurationen einsehen, soweit dem datenschutzrechtliche Gründe nicht entgegenstehen. Die Systembetreuer geben dem PR auf Wunsch Einblick in die Office 365 Administrator Konsole und erläutern die Berichte und Sicherheitseinstellungen in Office 365.

### **§ 7.5. Sanktionen**

im Falle eines Verstoßes gegen diese DV und die Durchführung einer nicht genehmigten Leistungs- und Verhaltenskontrolle hat der PR das Recht, die sofortige Abschaltung oder einen eingeschränkten Weiterbetrieb des IT-Systems zu verlangen, bis eine Einigung erreicht wurde. Der Schule verpflichtet sich, die Forderung des PR unverzüglich umzusetzen. Der PR hat das Recht, bei der Aufklärung des Sachverhalts umfassend informiert zu werden. Er hat darüber hinaus das Recht, eigenständige Untersuchungen durchzuführen, die der Aufklärung dienlich sind. Der Schule hat dem PR alle Informationen und Zugangsberechtigungen zur Verfügung zu stellen, die dieser für die Aufklärung des Sachverhalts benötigen.

## **§ 7.6. Schlichtungsstelle**

Kommt eine Einigung über die Einführung neuer Komponenten und Funktionen oder über die Auslegung dieser DV nicht zustande, so bilden Schule und PR ein Gremium mit jeweils 2 Mitgliedern (Schlichtungsstelle). Die Schlichtungsstelle tritt innerhalb von 2 Wochen auf Verlangen einer Betriebspartei zusammen, und verhandelt über den bestehenden Dissens. Entscheidungen werden mit einfacher Mehrheit getroffen.

Kommt innerhalb von 4 Wochen keine Einigung zustande, so kann jede Betriebspartei die Einigungsstelle anrufen. Die Betriebsparteien verpflichten sich, den Spruch der Einigungsstelle anzuerkennen und umzusetzen.

## **§ 8 Sicherstellen der Betriebssicherheit / Compliance**

### **§ 8.1. Administrative Nutzung von Protokolldaten**

Systemdaten und Protokolldateien dürfen ausschließlich für folgende Zwecke genutzt werden:

- Gewährleistung der Systemsicherheit,
- Nicht-personalisierte Feststellung der Nutzungsdauer und -häufigkeit,
- Analyse und Korrektur von technischen Fehlern im System,
- Optimierung der IT-Systeme,
- statistische Auswertungen ohne individuelle Kennung über Zugriff auf Ressourcen im Netz,
- Missbrauchskontrolle unter Beachtung der in dieser Vereinbarung niedergelegten Verfahren.

Weitere Auswertungen, außerhalb der in dieser Dienstvereinbarung festgelegten Berichte, sind nicht zulässig. Die Zugriffsberechtigung auf solche Daten wird nur den von der Schule bestellten und dem PR bekannten Systemadministratoren und externen Dienstleistern im Rahmen datenschutzrechtlich zulässiger Auftragsverarbeitungsverträge gewährt. Diese haben auf Grund privilegierter Zugriffsrechte Zugang zu personenbezogenen Daten und die Möglichkeit, den Umgang mit den Systemen zu kontrollieren oder in Statistiken zu erfassen.

Der Zugriff auf die entsprechenden Funktionen ist auf diejenigen Personen begrenzt, die für die Wartung der Hard- und Software sowie die Netzwerkadministration zuständig sind. Die entsprechenden Dateien werden nur so lange gespeichert, wie dies zur Erfüllung der oben genannten Zwecke und gesetzlicher Bestimmungen erforderlich ist. Office 365 kann automatisch Alarm- und Aufmerksamkeitsmeldungen an alle Administratoren schicken, die nur zum Zwecke der Erhaltung der Systemsicherheit und des Schutzes vor Schadware eingesetzt werden dürfen.

### **§ 8.2. Zulässige Auswertungen**

Sämtliche Auswertungen, die nicht der Systemsicherheit dienen (statistische Auswertungen) sind zu pseudonymisieren. Hierzu wird die entsprechende Funktion in Office 365 „In allen Berichten anonyme Bezeichner anstelle von Namen anzeigen“ eingeschaltet.

Die Berichte aus dem Office 365 Security & Compliance Center können für die unter § 8.1 genannten Zwecke personalisiert benutzt werden. Eine Verwendung der Berichte für arbeitsrechtliche Maßnahmen bleibt ausgeschlossen.

### **§ 8.3. Verpflichtung der Administratoren**

Jeder Inhaber einer administrativen Rolle oder Funktion in Office 365 wird zur Wahrung der Vertraulichkeit und des Datenschutzes geschult und schriftlich verpflichtet. Administratoren verpflichten sich, personenbezogene Daten selbst nicht ohne Befugnis zu verarbeiten und anderen Personen diese Daten nicht unbefugt mitteilen oder zugänglich machen. Sie werden insbesondere

verpflichtet, die datenschutzrechtlichen Vorgaben und Weisungen in der Schule zu beachten. Dies gilt insbesondere auch für die externen Dienstleister, die aufgrund eines bestehenden Auftragsverarbeitungsvertrags eine administrative Rolle oder Funktion in Office 365 innehaben.

## **§ 9 Löschfristen**

Die Office 365 Konten der Beschäftigten werden inklusive deren Inhalt 3 Monate nach Beendigung des Arbeitsverhältnisses eines Beschäftigten vollständig gelöscht. Auf Wunsch des Beschäftigten erfolgt dies auch zu einem früheren Zeitpunkt. Dies gilt nicht, wenn der Löschung gesetzliche Aufbewahrungsfristen entgegenstehen. Protokolldaten werden von Microsoft automatisch nach 90 Tagen gelöscht.

## **§ 10 Qualifizierung der Benutzer**

Die Nutzer der Anwendungen aus Office 365 werden auf ihre Arbeit im erforderlichen Maße, unterschieden nach Ihrer Funktion, vorbereitet.

Die Qualifizierungsmaßnahmen müssen über die für die Bedienung erforderlichen Kenntnisse hinaus einen Einblick in die Funktionsweise des Systems geben und seine Bedeutung innerhalb der schulischen Arbeitsabläufe und bezogen auf den jeweiligen Arbeitsplatz deutlich machen. Auch ist über die Bestimmungen des Datenschutzes sowie dieser Dienstvereinbarung zu schulen. Die Schule sichert zu, bestehende Mitbestimmungsrechte zur Schulungsplanung des Personalrats zu beachten. Die erforderlichen Kosten für die Schulungen / Einweisungen trägt die Schule nach Absprache mit dem Schulträger. Den Beschäftigten ist ausreichend Zeit und Gelegenheit zur Einarbeitung und zum Üben zu geben, gegebenenfalls an Schulungssystemen. Bei Bedarf werden Nachschulungen angeboten. Die Mitbestimmungsrechte des Betriebsrats sind zu wahren.

## **§ 11 Schlussbestimmungen**

### **§ 11.1. Inkrafttreten, Kündigung**

Diese Dienstvereinbarung tritt mit Unterzeichnung in Kraft. Die Dienstvereinbarung kann mit einer Frist von drei Monaten zum Ende Quartals gekündigt werden. Bis zum Abschluss einer neuen Vereinbarung gilt diese Dienstvereinbarung fort. Die Geltung aller weiteren Regelungen und Vereinbarungen insb. zum Thema IT bleibt unberührt.

### **§ 11.2. Salvatorische Klausel**

Sollte sich herausstellen, dass eine der vorstehenden Regelungen unwirksam ist, bleiben die übrigen bestehen. Anstelle der unwirksamen tritt eine Regelung, die der gewollten (unwirksamen) am nächsten kommt. Gleiches gilt, wenn eine getroffene Regelung unvollständig, widersprüchlich oder missverständlich ist. Treten Meinungsverschiedenheiten bezüglich der Auslegung oder Anwendung der Regelungen auf, entscheidet die Schlichtungsstelle gemäß § 7.6.

**Datum**

**Unterschrift Grace-Hopper-Gesamtschule**

**Unterschrift LR**

## Anhang A: Genutzte Office 365 Dienste

Dienstübergreifende Angaben für Löschfristen: Metadaten (Log-Dateien) werden automatisch nach 90 Tagen durch Microsoft gelöscht.

### Bezeichnung: Azure Active Directory, Azure Information Protection, Mehrfaktoranmeldung

Funktion	Das Azure Active Directory (AAD) ist der zentrale Verzeichnisdienst für alle Office 365 Anwendungen. Es dient in erster Linie zur Authentifizierung der Benutzer und der Registrierung von Geräten, um Single-Sign-On zu ermöglichen.
Verarbeitete Daten	Name, Vorname, Email-Adresse, Metadaten zu Anmeldungen und sicherheitsrelevanten Vorgängen (An-Abmeldungen, Rechteänderungen, etc)
Löschfristen	Benutzerkonten werden beim Ausscheiden eines Beschäftigten deaktiviert und nach 90 Tagen gelöscht.
Überwachungsprotokolle, Anmeldeberichte, Sicherheitsberichte	Dienen der Systemintegrität und Betriebssicherheit, werden nach 90 Tagen gelöscht, Zugriff nur Administratoren
Azure Information Protection	Ermöglicht für AAD-Gruppen eine zertifikatsbasierte Verschlüsselung von Dateien auf allen Endgeräten. Die Dateien können danach nur von Mitgliedern der Gruppe mit den eingestellten Rechten (Lesen oder/und Schreiben) geöffnet werden.
Mehrfaktoranmeldung	Nach Aktivierung erfordert die Anmeldung an Office 365 Dienste in gewissen zeitlichen Abständen die Angabe eines zweiten Faktors wie eine private E-Mailadresse, Telefonnummer, Beantwortung von Fragen oder die Microsoft Authenticator App.

### Bezeichnung: Exchange Online und ATP

Funktion	Exchange Online ist eine Groupware- und E-Mail-Transport-Server-Software. Sie dient der zentralen Ablage und Verwaltung von dienstlichen E-Mails, Terminen, Kontakten, Aufgaben und weiteren Elementen für mehrere Benutzer und ermöglicht so die Zusammenarbeit in einer Arbeitsgruppe oder in der gesamten Organisation.
Verarbeitete Daten	Name, Vorname, Email-Adresse, Inhaltsdaten von Email, Kalender und Kontakten, Metadaten zur Kommunikation und Produktnutzung
Löschfristen	Inhaltsdaten werden 90 Tage nach Ausscheiden eines Beschäftigten gelöscht.
Transportregeln	Dienen der Verhinderung von Weiterleitungen an private Konten und werden von den Administratoren erstellt
Postfachüberwachung	Es wird protokolliert, wenn ein Benutzer, bei dem es sich nicht um den Besitzer des Postfachs handelt, auf das Postfach zugreift, zwecks Sicherstellen der Systemintegrität und Vertraulichkeit, Zugriff nur Administratoren
Advanced Threat Protection (ATP)	Es wird jeder Link in E-Mails und Onedrive Dokumenten so umgeschrieben, dass er zum Zeitpunkt des Klicks noch einmal überprüft wird. Zusätzlich wird jeder Anhang in einem virtuellen Container nach aktiven Elementen, die Daten verändern würden, untersucht. Solche Anhänge werden gelöscht.
InPlace Hold, Verhindern von Datenverlust,	Diese Funktionen werden derzeit nicht genutzt

Aufbewahrungsrichtlinien und Journal	
--------------------------------------	--

#### Bezeichnung: Security & Compliance

Funktion:	Office 365 enthält eine Vielzahl von Funktionen, die dabei unterstützen sollen, die Systemsicherheit sowie die Compliance der Organisation sicherstellen zu können.
Verarbeitete Daten:	Name, Vorname, Email-Adresse, Weitere Profileigenschaften eines Benutzers, Metadaten zur Kommunikation und Produktnutzung
Berichte	zwecks Sicherstellen der Systemintegrität und Vertraulichkeit, Zugriff nur Administratoren
PowerBI, Bezeichnungen, Bezeichnungsrichtlinien, Verhindern von Datenverlust (DLP) Data Governance, Aufsicht und Inhaltssuche	Diese Funktionen werden derzeit nicht genutzt

#### Bezeichnung: SharePoint Online, OneDrive, Delve

Funktion	SharePoint Online wird indirekt durch Teams oder Office 365 Gruppen oder OneDrive genutzt für die Verwaltung der Zugriffsrechte, von Kalendern und Dokumentenbibliotheken
Verarbeitete Daten	Name, Vorname, Email-Adresse, weitere Profileigenschaften eines Benutzers, Inhaltsdaten von Dokumenten und Listen, Metadaten zur Verwendung und Produktnutzung
Löschfristen	In den Papierkorb verschobene Dokumente werden automatisch nach 30 Tagen gelöscht.
Benutzerprofile	enthalten Name, Vorname, Email-Adresse und ermöglichen Kommunikation und Zusammenarbeit. Jeder Beschäftigte kann freiwillig weitere Informationen hinzufügen und löschen.
OneDrive for Business	Dient der Ablage persönlicher Dokumente, die jeder selbst lesen, schreiben und löschen kann. Fälschlich gelöschte Dateien können über einen Zeitraum von maximal 4 Wochen selbst wieder hergestellt werden. Einzelne Dateien oder Ordner können anderen Benutzern zum Lesen oder zum Lesen und Schreiben freigegeben werden.
Delve	Dient dem leichteren Auffinden relevanter Dokumente und Informationen und zeigt zuletzt benutzte Daten an. Die Anzeige umfasst sowohl eigene Daten als auch durch andere Personen freigegebene Daten. Bei Bedenken bzgl. unbeabsichtigter Freigaben kann Delve von den Administratoren global ausgeschaltet werden.

**Bezeichnung: Teams**

Funktion	Microsoft Teams ist einerseits eine whatsapp-ähnliche Chatumgebung mit der Möglichkeit, private 1-zu-1 Chats zu führen und Dokumente und Daten einer Gruppe von Personen zur Verfügung zu stellen. Darüber hinaus ist es durch Einbindung der Klassennotizbücher eine auf OneNote und Formularen basierende Lernplattform mit dem das Lehrer/Schüler-Verhältnis angepassten Zugriffsrechten, Aufgabenzuteilung und Aufgabenbewertung.
Verarbeitete Daten	Name, Vorname, Email-Adresse, Weitere Profileigenschaften eines Benutzers, Präsenzinformationen, Metadaten zur Kommunikation und Produktnutzung, Inhalte der Klassennotizbücher.
Löschfristen	Teams mit Klassennotizbüchern der Lehrer und Schüler werden zum Schuljahresende inklusive aller gespeicherten Daten gelöscht.
Richtlinien	Teams inkludiert eine Übersetzungsfunktion, die derzeit noch auf US Servern ausgeführt wird und daher standardmäßig gesperrt ist.
Konnektoren und Apps	Diese Funktionen werden derzeit nicht genutzt

**Bezeichnung: Intune für Bildung**

Funktion	Intune ermöglicht mittels des Azure Active Directory die Verwaltung von Geräten, inklusive der Installation von Applikationen, Updates und Richtlinien für Windows 10, Mac OS, iOS und Android.
Verarbeitete Daten	Benutzerprofile inklusive zwischengespeicherter One-Drive Dateien, Namen der Rechner, benutzerbezogene Rechtezuweisung für die Nutzung von Geräteeigenschaften und -einstellungen
Löschfristen	Bedarfsabhängig werden Benutzerprofile automatisch gelöscht, da alle Daten in OneDrive gesichert sind. Administratoren können Geräte im Problemfall auf den Auslieferungszustand zurücksetzen.

Grace-Hopper-Gesamtschule

A5

Muster-Nutzungsordnung-Schule

# **Nutzungsordnung für das pädagogisches Netz der Grace-Hopper- Gesamtschule**

Liebe Schülerinnen und Schüler!

Für die Arbeit an der Schule steht Ihnen ein Zugang zum Internet, ein Microsoft Office 365 Konto mit verschiedenen Online-Diensten und Office ProPlus zur Nutzung für alle Arbeiten im Rahmen des Unterrichts zu Hause und in der Schule zur Verfügung. Alle Schülerinnen und Schüler werden gebeten, zu einem reibungslosen Betrieb beizutragen und die notwendigen Regeln einzuhalten.

Der besseren Verständlichkeit halber wird im Weiteren die grammatikalisch männliche Form verwendet, sie gilt aber in gleicher Weise unabhängig vom Geschlecht.

## **Allgemeine Rahmenbedingungen**

### **1. Datenschutz und Datensicherheit**

- Bitte beachten Sie, dass sich die Schule grundsätzlich über den Administrator Zugriff zu allen in Office 365 gespeicherten Daten verschaffen kann. Sie wird dies nur tun, wenn dies begründet ist, zum Beispiel ein Verdacht auf Missbrauch oder unangemessener Nutzung besteht oder dies für die Gewährleistung der technischen Sicherheit und Unversehrtheit der Daten notwendig erscheint. In jedem Fall werden die betroffenen Schülerinnen und Schüler und ggf. die Erziehungsberechtigten darüber informiert.

### **2. Passwörter**

- Wir richten für alle Schüler Office365-Konten mit einem Passwort ein, das Sie selbst ändern können.
- Bitte halten Sie das persönliche Passwort geheim. Sie könnten für missbräuchliche Verwendung Ihres Kontos zur Verantwortung gezogen werden.
- Es ist nicht statthaft, sich als ein anderer Schüler oder gar als Lehrer anzumelden.
- Vergessen Sie bitte nie, sich nach Beendigung der Nutzung von Ihrem Konto abzumelden. Dies dient Ihrer eigenen Sicherheit.

### **3. Bereitstellung und Nutzung von digitalen Materialien**

- Wenn Sie Daten in Office 365 ablegen und anderen Personen freigeben, achten Sie bitte darauf, dass Sie dazu berechtigt sind. Es könnte sein, dass der Urheber der Daten eine Weitergabe nicht gestattet. Sie sind dafür verantwortlich, die Bestimmungen des Urheberrechts einzuhalten.
- Wenn Sie Daten aus dem Internet im Zusammenhang mit dem Unterricht einsetzen, achten Sie bitte darauf, die Quelle der Information oder der Daten sorgfältig anzugeben.
- Sollten Sie Kenntnis erlangen, dass rechtswidrige Inhalte wie gestohlene Musik oder Filme oder Inhalte, die Gewalt, Hass und Hetze verbreiten, gespeichert oder geteilt werden, informieren Sie bitte sofort eine Lehrkraft Ihres Vertrauens oder den Datenschutzbeauftragten der Schule Herr Torsten Leis.



#### 4. Nutzung von Informationen aus dem Internet

- Der Internet-Zugang soll grundsätzlich nur für Zwecke genutzt werden, die einem schulischem Zweck dienen. Hierzu zählt auch ein elektronischer Informationsaustausch, der unter Berücksichtigung seines Inhalts und des Adressatenkreises mit dem Unterricht an der Schule im Zusammenhang steht.
- Die Nutzung von weiteren Anwendungen (z.B. durch Herunterladen aus dem Internet) muss im Zusammenhang des Unterrichts stehen.
- Im Namen der Schule dürfen weder Vertragsverhältnisse eingegangen noch kostenpflichtige Dienste im Internet benutzt werden.
- Die Schulleitung ist nicht für den Inhalt der über Ihren Internet-Zugang abrufbaren Angebote verantwortlich.

#### 5. Verbotene Nutzungen

- Es ist verboten, pornographische, gewaltverherrlichende oder rassistische Inhalte aufzurufen oder zu versenden. Werden solche Inhalte versehentlich aufgerufen, ist die Anwendung zu schließen.

#### 6. Eingriffe in die Hard- und Softwareinstallation

- Veränderungen der Installation und Konfiguration der Arbeitsstationen und des Netzwerkes sowie Manipulationen an der Hardwareausstattung sind grundsätzlich untersagt.
- Bitte vermeiden Sie unnötiges Datenaufkommen durch Laden und Versenden von großen Dateien (zum Beispiel Grafiken, Videos, etc.)

#### 7. Schutz der Geräte

- Die Bedienung der Hard- und Software hat entsprechend der Instruktionen zu erfolgen. Störungen oder Schäden sind sofort der für die Computernutzung verantwortlichen Person oder dem Systembetreuer Herr Maik Vogler zu melden. Wer schuldhaft Schäden verursacht, muss für deren Behebung aufkommen.
- Die Tastaturen sind durch Schmutz und Flüssigkeiten besonders gefährdet, deshalb ist in den Computerräumen Essen und Trinken grundsätzlich verboten.

#### 9. WLAN Zugang

- Die Authentifizierung erfolgt bei schuleigenen Geräten (Notebooks, Tablets, etc.) über einen WPA2 Zugang. Die Zugangsdaten wurden in den schuleigenen Geräten gespeichert.
- Die Nutzung des WLANs erfolgt in der Regel nur zu schulischen Zwecken.

### Lernplattform Office 365 Education

An unserer Schule wird Office365 Education als Lern – und Kommunikationsplattform eingeführt. Diese Plattform ist für die Nutzer kostenlos und ermöglicht eine unserem Medienkonzept entsprechend moderne und zukunftsweisende Zusammenarbeit zwischen den Lehrenden und Lernenden.

Dem Benutzer wird dabei während seiner Schulzeit ein Benutzerkonto auf der Online-Plattform Office 365 Education zur Verfügung gestellt. Der Zugriff auf diese Dienste erfolgt über die Seite <https://portal.office.com> oder alternativ über die Seite <https://teams.microsoft.com>.

- Eine E-Mail-Adresse und ein 50 GB großes Postfach
- Die Bereitstellung des aktuellen Microsoft Office-365 ProPlus Pakets (Outlook, Word, PowerPoint, Excel, OneDrive) zum kostenlosen Herunterladen und Betreiben auf bis zu 10 heimischen Geräten
- Die Bereitstellung des Cloudspeichers OneDrive der Schule mit 1 TB Datenspeicher
- Die chat-basierte Lernplattform Teams, die jedem Schüler für jedes Fach ein eigenes OneNote Notizbuch zur Verfügung stellt, und die Ablage von Daten und Dokumenten ermöglicht.

Die Schule behält sich vor, einzelne Dienste nicht zur Verfügung zu stellen. Beim Verlassen der Schule wird das Benutzerkonto deaktiviert und gelöscht. Alle vorhandenen Daten werden zu diesem Zeitpunkt ebenfalls gelöscht.

Die Einführung von Office 365 in unserer Schule ist datenschutzrechtlich geprüft und wurde von der Schulleitung, den Vertretern der Lehrer, der Eltern und der Schüler zum 01.08.2020 genehmigt. Die von Schülern oder Lehrern in Office 365 abgelegten Daten werden ausschließlich innerhalb der EU gespeichert, sie werden weder durchsucht noch an Dritte weitergegeben.

## **Schlussvorschriften**

Die Schülerinnen und Schüler werden zu Beginn der schulischen Nutzung über diese Nutzungsordnung unterrichtet. Sie versichern durch ihre Unterschrift, dass sie diese anerkennen. Diese Belehrung wird im Schultagebuch protokolliert und jedes Jahr, zu Beginn des Schuljahres, wiederholt. Diese Benutzerordnung ist Bestandteil der jeweils gültigen Hausordnung und tritt am Tage nach ihrer Bekanntgabe an der Schule in Kraft.

Zu widerhandlungen gegen diese Nutzungsordnung können den Entzug der Nutzungsberechtigung und ggf. rechtliche Konsequenzen und die unverzügliche Pflicht zur Rückgabe der überlassenen Soft- und Hardware zur Folge haben.

## Erklärung

Am \_\_\_\_\_ wurde ich in die Nutzungsordnung zur Computer- und Internet-Nutzung eingewiesen.

Mit den festgelegten Regeln bin ich einverstanden. Sollte ich gegen die Nutzungsregeln verstoßen, verliere ich meine Nutzungsberechtigung und muss mit dienstrechtlichen/schulrechtlichen Maßnahmen rechnen. Bei Verstoß gegen gesetzliche Bestimmungen sind weitere zivil- oder strafrechtliche Folgen nicht auszuschließen.

\_\_\_\_\_  
Klasse

\_\_\_\_\_  
Name der Schülerin / des Schülers (in Druckbuchstaben)

\_\_\_\_\_  
Ort / Datum

\_\_\_\_\_  
Unterschrift der Schülerin / des Schülers

\_\_\_\_\_  
Ort / Datum

\_\_\_\_\_  
Unterschrift Erziehungsberechtigter

Grace-Hopper-Gesamtschule

A5

Nutzungsordnung

# Nutzungsordnung für das „pädagogisches Netz“ der Grace-Hopper-Gesamtschule inklusive Office 365

Für die Arbeit an der Schule steht Ihnen ein Zugang zum Internet, ein E-Mail-Account und Office 365 zur dienstlichen/schulischen Nutzung für alle Arbeiten im Rahmen des Unterrichts zur Verfügung. Alle Beteiligten sind aufgefordert zu einem reibungslosen Betrieb beizutragen und die notwendigen Regeln einzuhalten.

## Allgemeine Rahmenbedingungen

### 1. Datenschutz und Datensicherheit

- Die gesetzlichen Bestimmungen des Datenschutzes, Strafrechts und des Jugendschutzrechts sind zu beachten.
- Die Schulleitung / der Netzwerkbeauftragte ist in der Wahrnehmung seiner Dienstaufsichtspflicht berechtigt, den Datenverkehr zu speichern und zu kontrollieren.
- Die Fachlehrerin / der Fachlehrer hat im Rahmen seiner Aufsichtspflicht und zu unterrichtlichen Zwecken die Berechtigung auf Daten der Schülerinnen und Schüler zu zugreifen.
- Diese Daten werden in der Regel nach einem Monat, spätestens jedoch zu Beginn eines jeden neuen Schuljahres gelöscht. Dies gilt nicht, wenn Tatsachen den Verdacht eines schwerwiegenden Missbrauchs der Computer und mobilen Geräte begründen. Die Schulleitung wird von seinen Einsichtsrechten nur in Fällen des Verdachts von Missbrauch und durch verdachtsunabhängige Stichproben Gebrauch machen.
- Die Schulleitung sichert weiter zu, dass der Datenverkehr nicht statistisch ausgewertet wird.

### 2. Passwörter

- Vor der ersten Benutzung muss gegebenenfalls das eigene Benutzerkonto, der Account, freigeschaltet werden; ohne individuelles Passwort darf die vernetzte Umgebung (lokales Netz und/oder Office 365) nicht genutzt werden.
- Das persönliche Passwort ist geheim zu halten.
- Es ist den Schülerinnen und Schülern nicht gestattet, sich als ein andere(r) Schüler(in) oder gar als Lehrer(in) anzumelden.
- Der Zugang sollte aus datenschutzrechtlichen Gründen nur mit einem sicheren, nicht trivialen, persönlichen Passwort genutzt werden.
- Die Hinweise des Bundesamt für Sicherheit und Informationstechnik:  
[https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSIFB/sichere\\_passwoerter\\_faktenblatt.pdf?\\_\\_blob=publicationFile&v=12](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSIFB/sichere_passwoerter_faktenblatt.pdf?__blob=publicationFile&v=12)
- Nach Beendigung der Nutzung melden Sie sich vom Netz und am PC ab.

### 3. Bereitstellung und Nutzung von „Digitalisaten“ (digitalen Materialien) nach § 52a UrhG

- Sie halten die geltenden rechtlichen Bestimmungen, insbesondere des Urheberrechtes und des Datenschutzes ein (siehe <http://www.bpb.de/gesellschaft/medien-und-sport/urheberrecht/169992/urheberrecht-in-schule-und-ausbildung>).
- Die Person, die Materialien im pädagogischen Netz (Intranet) oder im Internet bereitstellt, ist für die Einhaltung der gesetzlichen Bestimmungen des Urheberrechts und der Gesamtverträge verantwortlich.
- Sollten Sie Kenntnis erlangt haben, dass rechtswidrige Inhalte im pädagogischen Netz (Intranet) gespeichert werden, werden Sie die zuständige Lehrkraft unverzüglich darüber informieren.
- Materialien, die entsprechend § 52a UrhG bereitgestellt werden, dürfen ausschließlich im Rahmen des Unterrichts genutzt werden. Eine darüber hinaus gehende Nutzung (kopieren/vervielfältigen) ist verboten.
- Die Veröffentlichung von fremden Inhalten (Fotos und Materialien) im Internet ist nur mit der Genehmigung des Urhebers gestattet. So dürfen z. B. Texte, gescannte Bilder oder onlinebezogene Materialien nur mit Erlaubnis der Urheber in eigenen
- Internetseiten verwandt werden. Der Urheber ist zu nennen, wenn dieser es wünscht.
- Auch bei der Weiterverarbeitung sind Urheber- oder Nutzungsrechte zu beachten.

### 4. Nutzung von Informationen aus dem Internet

- Der Internet-Zugang soll grundsätzlich nur für Zwecke genutzt werden, die dienstlichem/schulischem Zweck dienen. Hierzu zählt auch ein elektronischer Informationsaustausch, der unter Berücksichtigung seines Inhalts und des
- Adressatenkreises mit dem Unterricht an der Schule im Zusammenhang steht.
- Die Nutzung von weiteren Anwendungen (z.B. durch Herunterladen aus dem Internet) muss im Zusammenhang des Unterrichts stehen.
- Im Namen der Schule dürfen weder Vertragsverhältnisse eingegangen noch kostenpflichtige Dienste im Internet benutzt werden.
- Die Schulleitung ist nicht für den Inhalt der über Ihren Internet-Zugang abrufbaren Angebote verantwortlich. Die Veröffentlichung von frei zugänglichen Internetseiten bedarf der Genehmigung durch die Schulleitung.

### 5. Verbotene Nutzungen

- Es ist verboten, pornographische, gewaltverherrlichende oder rassistische Inhalte aufzurufen oder zu versenden. Werden solche Inhalte versehentlich aufgerufen, ist die Anwendung zu schließen.

- Nutzer, die unbefugt Software von den Arbeitsstationen oder aus dem Netz kopieren oder verbotene Inhalte nutzen, machen sich strafbar und können zivil- oder strafrechtlich verfolgt werden.

## 6. Eingriffe in die Hard- und Softwareinstallation

- Veränderungen der Installation und Konfiguration der Arbeitsstationen und des Netzwerkes sowie Manipulationen an der Hardwareausstattung sind grundsätzlich untersagt.
- Unnötiges Datenaufkommen durch Laden und Versenden von großen Dateien (zum Beispiel Grafiken, Videos, etc.) aus dem Internet ist zu vermeiden. Sollte eine Nutzerin oder ein Nutzer unberechtigt größere Datenmengen in seinem Arbeitsbereich ablegen, ist die Schule berechtigt, diese Daten zu löschen.
- Die ständige Synchronisation von einer Cloud (z.B. OneDrive) mit Schulgeräten muss abgeschaltet werden, damit unser Netz nicht unnötig belastet wird.

## 7. Schutz der Geräte

- Die Bedienung der Hard- und Software hat entsprechend der Instruktionen zu erfolgen. Störungen oder Schäden sind sofort der für die Computernutzung verantwortlichen Person zu melden. Wer schuldhaft Schäden verursacht, hat diese zu ersetzen.
- Die Tastaturen sind durch Schmutz und Flüssigkeiten besonders gefährdet, deshalb ist in den Computerräumen Essen und Trinken grundsätzlich verboten.

# Schulregelungen

## 8. Zugang zum pädagogischen Netz

- Für die Dauer der Schulzugehörigkeit erhalten Sie für dienstliche / schulische Zwecke einen persönlichen Account, der mit einem individuellen Passwort geschützt werden muss.
- Über diesen Zugang können Sie sich am pädagogischen Netz anmelden und folgende Dienste nutzen
  - Arbeiten im pädagogischen Netz, Programme nutzen, Zugriff auf Unterlagen im Zusammenhang mit dem Unterricht, Austausch von Materialien
  - Abruf von dienstlichen / schulischen E-Mails
  - Zugang zu Schul-Servern
  - Zugang zum WLAN an schuleigenen Geräten

## 9. Schul-Server und schulische Email-Adressen

### 9a) Umfang und Laufzeit:

Ab März 2018 wird an der Grace-Hopper-Gesamtschule Office365 Education als Online-Kommunikationsplattform eingeführt. Diese Plattform ist für die Nutzer kostenlos und ermöglicht eine unserem neuen Medienkonzept entsprechend moderne und zukunftsweisende Zusammenarbeit zwischen den Lehrenden und Lernenden.

Dem Benutzer wird dabei während seiner Schulzeit ein Benutzerkonto auf dem Schulserver sowie im Internet auf der Online-Plattform Office 365 Education zur Verfügung gestellt. Der Zugriff auf diese Dienste erfolgt über die Seite <https://login.microsoftonline.com>. Dazu gehört die für den Nutzer, nicht aber für die Schule kostenfreie Nutzung von verschiedenen Diensten.

- Eine schulische E-Mail-Adresse
- Microsoft Office Online (Outlook Online, PowerPoint Online, Word Online, Online Speicherplatz auf OneDrive)
- Die Bereitstellung des aktuellen Microsoft Office-Pakets (Outlook, Word, PowerPoint, Excel, Access, Publisher, Skype for Business, OneDrive) zum kostenlosen Herunterladen und Betreiben auf bis zu 5 heimischen Geräten

Die Anzahl der zur Verfügung stehenden Lizenzen ist begrenzt; die Grace-Hopper-Gesamtschule behält sich vor, einzelne Dienste nicht zur Verfügung zu stellen. Beim Verlassen der Schule wird das Benutzerkonto deaktiviert und gelöscht. Alle vorhandenen Daten werden zu diesem Zeitpunkt ebenfalls gelöscht.

### 9b) Verhaltensregeln, Rechtsverstöße und Datenschutz

In erster Instanz gilt das Service Agreement von Microsoft und insbesondere auch der darin enthaltene Verhaltenskodex, der einen freundlichen und fairen Umgang aller

Beteiligten miteinander regelt. Dieses ist hier abzurufen:

<https://www.microsoft.com/de-de/servicesagreement/>

Die Grace-Hopper-Gesamtschule duldet keine Verstöße gegen die bestehende Gesetzgebung. Verstöße werden an die jeweiligen Behörden weitergeleitet und geahndet. Dies betrifft speziell folgende Themen:

- Tausch von illegalen Daten, z.B. Tauschbörsen
- Verletzung der Privatsphäre
- Formen des Cybermobbings, wie z.B.
  - Beleidigungen,
  - Verleumdung,
  - Üble Nachrede, ○
  - Nachstellungen, ○
  - Hasstiraden und
  - Beschimpfungen.



Die Grace-Hopper-Gesamtschule nutzt Webservices von Microsoft. Um die Online-Accounts zu erstellen, werden Schülerdaten in Form von Vor-/Nachname und Klasse an Microsoft übermittelt. Ansonsten werden keine personenbezogenen Daten übermittelt. Damit die Vorschriften des Datenschutz-Gesetzes eingehalten werden, müssen Schüler und Erziehungsberechtigte dieser Übermittlung zustimmen. Des Weiteren gilt die europäische und deutsche Gesetzgebung.

## **10. WLAN Zugang**

- Die Authentifizierung erfolgt bei schuleigenen Geräten (Notebooks, Tablets, etc.) über einen WPA2 Zugang. Die Zugangsdaten wurden in den schuleigenen Geräten gespeichert.
- Die Nutzung des WLANs erfolgt in der Regel nur zu schulischen Zwecken.

## **11. Schlussvorschriften**

Die Schülerinnen und Schüler werden zu Beginn der schulischen Nutzung über diese Nutzungsordnung unterrichtet. Sie versichern durch ihre Unterschrift, dass sie diese anerkennen. Diese Belehrung wird im Schultagebuch protokolliert und jedes Jahr, zu Beginn des Schuljahres, wiederholt. Diese Benutzerordnung ist Bestandteil der jeweils gültigen Hausordnung und tritt am Tage nach ihrer Bekanntgabe an der Schule in Kraft.

Zu widerhandlungen gegen diese Nutzungsordnung können den Entzug der Nutzungsberechtigung und ggf. rechtliche Konsequenzen und die unverzügliche Pflicht zur Rückgabe der überlassenen Soft- und Hardware zur Folge haben.

## Erklärung

Am \_\_\_\_\_ wurde ich in die Nutzungsordnung zur Computer- und Internet-Nutzung eingewiesen.

Mit den festgelegten Regeln bin ich einverstanden. Sollte ich gegen die Nutzungsregeln verstoßen, verliere ich meine Nutzungsberechtigung und muss mit dienstrechtlichen/schulrechtlichen Maßnahmen rechnen. Bei Verstoß gegen gesetzliche Bestimmungen sind weitere zivil- oder strafrechtliche Folgen nicht auszuschließen.

\_\_\_\_\_  
Klasse

\_\_\_\_\_  
Name der Schülerin / des Schülers (in Druckbuchstaben)

\_\_\_\_\_  
Ort / Datum

\_\_\_\_\_  
Unterschrift der Schülerin / des Schülers

\_\_\_\_\_  
Ort / Datum

\_\_\_\_\_  
Unterschrift Erziehungsberechtigter

Grace-Hopper-Gesamtschule

A6

Einwilligung Schule

## **Einwilligungserklärung nach DSGVO Art. 6 (1) a zur Nutzung des Microsoft Unternehmens-Cloud Dienstes Office 365**

Alle Mitarbeiter und Schüler können die IT-Infrastruktur der Schule nutzen. Zusätzlich zur lokalen Infrastruktur der Schule können Sie freiwillig zusätzlich folgende Komponenten nutzen:

Eine moderne Groupware für E-Mail, Datenablage und chat-basierte Kommunikation, in der als Zugangsdaten Ihr Vorname, Nachname, Anzeigename und E-Mailadresse gespeichert werden. Diese Daten liegen jedoch nicht auf lokalen Servern, sondern im Rahmen des Unternehmens-Cloud-Dienstes Office 365 in EU Rechenzentren von Microsoft.

Es ist vertraglich gesichert, dass Ihre Nutz-Daten den EU Raum nicht verlassen und sie von Microsoft in keiner Weise ausgewertet oder gelesen werden können. Der Auftragsverarbeitungsvertrag, den der Schulträger mit Microsoft Irland abgeschlossen hat, enthält die EU Datenschutzklauseln, der RZ Betrieb von Microsoft ist nach den Datenschutzrichtlinien ISO 27018 zertifiziert, alle Daten sind maschinell verschlüsselt. Die Nutzung von Office 365 ist unter der Maßgabe der Freiwilligkeit konform mit der Datenschutzgrundverordnung. Die Übermittlung der personenbezogenen Daten für das notwendige Konto bei Office 365 wurde von unserem Datenschutzbeauftragten, Herrn Torsten Leis geprüft und als bedenklich eingestuft.

Nähere Informationen zu Office 365 und den datenschutzrechtlichen Angaben finden Sie unter <http://www.trustcenter.office365.de>. Zur Unterstützung bei der Konfiguration, Verwaltung und Anlage der Office 365 Konten haben wir zusätzlich einen Auftragsverarbeitungsvertrag mit ES EUREGIO SYSTEMS GmbH abgeschlossen. Sie können die Unterlagen zur Auswahl des Verfahrens sowie die geschlossenen Verträge jederzeit beim Datenschutzbeauftragten einsehen.

Die Nutzung von Office 365 ist freiwillig. Gemäß § 17 DSGVO können Sie jederzeit gegenüber der Schulleitung die Berichtigung, Löschung und Sperrung Ihrer personenbezogenen Daten verlangen. Sie können darüber hinaus jederzeit ohne Angabe von Gründen die erteilte Einwilligungserklärung mit Wirkung für die Zukunft abändern oder gänzlich widerrufen, indem Sie dies unserem Datenschutzbeauftragten mündlich oder schriftlich mitteilen.

**Ich willige ein, dass mein Vorname, Nachname und Anmeldename zum Cloud-Dienst Office 365 übertragen und mit diesen Daten ein Nutzer-Konto mit E-Mailadresse angelegt wird. Zusätzlich willige ich ein, dass diese Angaben für die anderen Mitglieder der Schule, die Nutzer-Konten in derselben Office 365 Instanz haben, sichtbar sind.**

**Ort, Datum**

**Name**

**Unterschrift**

Grace-Hopper-Gesamtschule

A6

Eirwilligung

## Einwilligungserklärung zur Übermittlung Ihrer Zugangsdaten zum Microsoft Cloud Dienst Office 365

Alle Mitarbeiter und Schüler können die IT-Infrastruktur der Schule nutzen. Diese Infrastruktur besteht derzeit aus mehreren Komponenten:

1) einem lokalen Verzeichnisdienst, in dem der Name, Kontoname, Emailadressen, Büro und Telefonnummer der Mitarbeiter und Schüler gespeichert wird. Dieser Verzeichnisdienst läuft auf Servern in den Räumen der Schule und ermöglicht eine Anmeldung an den Rechnern in der Schule. An diesen Verzeichnisdienst sind weitere Dienste angeschlossen, nämlich (bitte angeben) ein E-Mail-Server für die Nutzung der E-Mail, ein Dateiserver zur Speicherung der dienstlichen Daten und Dokumente und ....

Es bestehen keine datenschutzrechtliche oder ISO Zertifizierung des Serverbetriebs. Die Schule übernimmt keine Garantie für die Sicherheit der Daten. Administrativen Zugriff auf die Daten haben Systembetreuer an unserer Schule und der Dienstleister (Firma), mit dem ein Auftragsverarbeitungsvertrag besteht. Ihre Daten werden nicht automatisch ausgewertet und nicht an Dritte weitergegeben. Drei Monate nach Beendigung Ihrer Beschäftigung werden diese Daten unwiderruflich gelöscht.

2) moderne Groupware für Email, Datenablage und chat-basierte Kommunikation, in der dieselben Zugangsdaten wie im lokalen Verzeichnisdienst gespeichert werden. Diese Daten liegen jedoch nicht auf lokalen Servern, sondern im Rahmen des Cloud-Dienstes Office 365 in EU Rechenzentren von Microsoft. Es ist vertraglich gesichert, dass Ihre Daten den EU Raum nicht verlassen und sie von Microsoft in keiner Weise verarbeitet werden können. Der Auftragsverarbeitungsvertrag, den die Schule mit Microsoft Irland abgeschlossen hat, enthält die EU Datenschutzklauseln. Der RZ-Betrieb von Microsoft ist nach den Datenschutzrichtlinien ISO 27018 zertifiziert, alle Daten sind maschinell verschlüsselt. Die Nutzung von Office 365 ist unter der Maßgabe der Freiwilligkeit konform mit der Datenschutzgrundverordnung. Die Übermittlung der personenbezogenen Daten für das notwendige Konto bei Office 365 wurde von unserem Datenschutzbeauftragten geprüft. Dazu gehören Anmeldenamen, Vor-/Nachname, Klasse und Rolle an unserer Schule. Nähere Informationen zu Office 365 und den datenschutzrechtlichen Angaben finden Sie unter <http://www.trustcenter.office365.de>. Zur Unterstützung bei der Konfiguration, Verwaltung und Anlage der Office 365 Konten haben wir zusätzlich einen Auftragsverarbeitungsvertrag mit <Dienstleister> abgeschlossen. Sie können die Unterlagen zur Auswahl des Verfahrens sowie die geschlossenen Verträge jederzeit beim Datenschutzbeauftragten einsehen.

Die Nutzung von Office 365 ist freiwillig. Gemäß § 17 DSGVO können Sie jederzeit gegenüber der Schulleitung die Berichtigung, Löschung und Sperrung Ihrer personenbezogenen Daten verlangen. Sie können darüber hinaus jederzeit ohne Angabe von Gründen die erteilte Einwilligungserklärung mit Wirkung für die Zukunft abändern oder gänzlich widerrufen, indem Sie dies unserem Datenschutzbeauftragten mündlich oder schriftlich mitteilen.

Ich willige ein, dass mein Vorname, Nachname und Anmeldenamen zum Cloud-Dienst Office 365 übertragen und mit diesen Daten ein Nutzer-Konto mit E-Mailadresse angelegt wird. Zusätzlich willige ich ein, dass diese Angaben für die anderen Mitglieder der Schule, die Nutzer-Konten in derselben Office 365 Instanz haben, sichtbar sind.

Datum	Ort	Vor-/Nachname	Unterschrift

A7

Technische und Organisatorische Maßnahmen für Verantwortliche

## Technische und Organisatorische Maßnahmen für Verantwortliche

Der Verantwortliche bestätigt, folgende Maßnahmen zur Einhaltung der Anforderungen an die Sicherheit der Datenverarbeitung ergriffen zu haben:

1. **Zugangskontrolle:** Videoüberwachung, Türsicherung, Sicherheitsschlösser, abschließbare Serverschränke, Alarmanlage, Schließsystem.
2. **Datenträgerkontrolle:** sichere Aufbewahrung, Verschlüsselung, ordnungsgemäße Vernichtung nach DIN 32757, Richtlinie an Mitarbeiter, keine Veränderungen vorzunehmen.
3. **Benutzerkontrolle:** Festlegung der Zugangsberechtigung, Authentifikation, Passwortvergabe, regelmäßige Kontrolle, Sperrung von Berechtigungen ausscheidender Mitarbeiter, Richtlinie zur Internetnutzung.
4. **Zugriffskontrolle:** Verwaltung durch Systemadministratoren, Nachvollziehbarkeit der Zugriffe, Festlegung differenzierter Berechtigungen in den IT-Systemen, Passwortrichtlinie inkl. Passwortlänge, Protokollierung von Zugriffen auf Anwendungen.
5. **Datenintegrität:** Erstellen eines Backupkonzepts, Antivirensoftware, Firewall und IDS, Erstellen eines Notfallplans.
6. **Transportkontrolle:** Verschlüsselung, Pseudonymisierung.
7. **Trennungskontrolle:** Richtlinie zur Trennung der DV unter Beachtung der Zweckbindung, keine Verwendung zu Werbezwecken etc.
8. **Mitarbeiterschulung**

---

Datum

---

Unterschrift Verantwortlicher



## Häufige Fragen und Antworten durch Kollegen, Eltern und Schüler

### Darf die Schule Office 365 einsetzen?

Ja, sie darf. Die Bildungseinrichtung (oder der Schulträger) schließt einen Vertrag zur Auftragsverarbeitung mit Microsoft Irland gemäß DSGVO ab, der die EU Standardvertragsklauseln enthält. Diese werden von auch allen Subunternehmen auferlegt. Damit ist Microsoft Irland gleichgestellt mit EU Anbietern. Die Speicherung der Nutzdaten erfolgt nur innerhalb der EU und die Daten verlassen die EU nicht. Microsoft Rechenzentren werden laufend nach strengsten internationalen Standards zertifiziert, sowohl nach ISO 27001, 27002, als auch nach dem Datenschutzstandard ISO 27018. Alle Nutzdaten sind server- und verbindungsseitig verschlüsselt. Weitere Auskünfte erteilt gerne unser Datenschutzverantwortlicher.

Verwechseln Sie bitte nicht die Organisations-Cloud Office 365 mit den Privatkundenangeboten von Microsoft. Letztere sind nicht geeignet für den Einsatz in einer Schule.

### Was macht Microsoft mit den Daten?

- Microsoft gibt für die Unternehmenscloud Office 365 weder Daten weiter noch werden sie inhaltlich in irgendeiner Art und Weise ausgewertet.
- Das Angebot ist strikt werbefrei.
- Die Microsoft Rechenzentren für deutsche Kunden liegen in Deutschland (Frankfurt und Berlin). Die Daten in den Rechenzentren sind in mehreren Ebenen verschlüsselt.
- Microsoft ermöglicht dem Nutzer von Office 365 eine Ende-zu-Ende Verschlüsselung, Mehrfaktor-Anmeldung, besonderen Schutz gegen gefährliche Anhänge in E-Mails und gegen gefälschten Links in Daten
- Die Nutzdaten bleiben immer in Deutschland gespeichert und verlassen somit die EU nicht.
- Der Datentransfer zu Office 365 ist Verbindungstechnisch verschlüsselt und zusätzlich innerhalb und zwischen den Rechenzentren verschlüsselt.
- Weitere Auskünfte erteilt gerne unser Datenschutzverantwortlicher.

### Wer sieht die Anmeldedaten?

Der Anmeldename in Office 365 wird auf allen Anmeldeservern von Microsoft weltweit gespeichert, damit Sie auch im Nicht-EU Ausland auf Ihre Daten zugreifen können. Alle weiteren Daten verlassen jedoch die EU nicht.

Microsoft Supportingenieure aus der EU erhalten nur nach expliziter Anforderung durch unseren Systembetreuer Zugriff auf Daten, um ein technisches Problem zu lösen. Supportingenieure außerhalb der EU können technisch durch die sog. Lock-Box-Technologie keinen Zugriff auf Office 365 Instanzen der EU erhalten.

Weitere Auskünfte erteilt gerne unser Datenschutzverantwortlicher.

## Ich habe gehört, dass der Cloud-Act US-Behörden Zugriff auf unsere Daten ermöglicht

Das ist nicht richtig. Der Cloud-Act regelt das Recht eines normalen Zivilgerichts der USA, Daten im Rahmen eines Strafverfahrens z. B. von Microsoft oder einer anderen Firma in der Welt direkt zu erbitten statt über ein Rechtshilfeverfahren, das Jahre dauert und nicht mehr zeitgemäß ist. EU Bürger sind davon nicht betroffen (solange Sie nicht in USA strafbar werden). Weitere Auskünfte erteilt gerne unser Datenschutzverantwortlicher.

## Ich habe gehört, dass Microsoft meine Daten ausspäht

Das ist nicht richtig. Jeder Hersteller von Software, die über das Internet bezogen oder genutzt wird, benötigt zur Vertragserfüllung Daten, mit der die korrekte und sichere Funktion der Software sichergestellt werden kann. Das gilt für jedes Betriebssystem, für jeden Browser, egal ob Open-Source oder kommerziell. Microsoft speziell überträgt niemals Nutzerdaten ohne Kenntnis und Zustimmung des Betroffenen und dokumentiert sehr sorgfältig, welche Telemetriedaten für welchen Zweck übertragen werden. Weitere Auskünfte erteilt gerne unser Datenschutzverantwortlicher.