Rahmen-Dienstvereinbarung

zwischen

Musterschule, Adresse

nachfolgend mit „Schule“ bezeichnet,

und

dem Personalrat der Musterschule

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 umfassen 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 Schule** **Unterschrift PR**

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. Zustätzlich 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 dan 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.