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)	**Städtische Realschule Heiligenhaus** Feldstr. 2, 42579 Heiligenhaus sekretariat@realschule-heiligenhaus.de 02056-6211
Falls zutreffend: Angaben zu weiteren gemeinsam für die Verarbeitung Verantwortlichen (jeweils Bezeichnung, Anschrift, E-Mail-Adresse und Telefonnummer)	
Datum der Einführung	01.10.2020
Stand dieser Dokumentation	Januar 2021
Behördlicher Datenschutzbeauftragter (Name, dienstliche Anschrift, E-Mail-Adresse, Telefonnummer)	Joachim Kroeske datenschutz_in_schulen@kreis-mettmann.de

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

Zweck	• IT-gestützte Zusammenarbeit der Mitarbeiter und Schüler der Schule mittels der Microsoft Office 365 Dienste Exchange Online, Sharepoint Online und der Lernplattform Teams. • 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. Besonders sind dies: - E-Mailkommunikation mit Termin- und Ressourcenverwaltung, gemeinsame Kalender, Office 365 Gruppen - Bereitstellung und Austausch von Dokumenten - Projektverwaltung zur Organisation der schulischen Abläufe, Chatfunktion - Lernplattform Teams mit Klassennotizbüchern, Bereitstellung von Unterrichtsmaterialien, Aufgaben mit Terminabgabe, Bewertung, Rückmeldung - Nutzung der Desktopversion von Office
Name des eingesetzten Verfahrens	Microsoft Office 365 (http://aka.ms/Wkcowi)
Dienstbeschreibungen	https://www.microsoft.com/de-de/licensing/product-licensing/products.aspx und https://technet.microsoft.com/en-us/library/office-365-service-descriptions.aspx

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	• Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, E-Mailadresse, weitere dienstliche E-Mailadressen, Funktion, dienstliche Telefonnummer falls bestehend) • Gruppenzugehörigkeiten in Teams, Mitbesitzer eines Teams, unterrichtete Fächer, unterrichtete Klassen
Daten der Schüler	• Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, Funktion) • Schulart, Klasse, Jahrgangsstufe • Besuchte Unterrichtseinheiten, für die Teams eingerichtet werden • Unterrichtselemente (Lehrstoff, Leistungserhebungen, Aufgabenzuteilungen, Bewertungen)
Daten aller Nutzer	• Grunddaten (Name, Vornamen, Anzeigename, Anmeldename, Funktion) • Berechtigungen • Log-Daten (Datum der letzten Passwortänderung, Datum der letzten Anmeldung, Größe und Zahl der gespeicherten Daten) • Historisierung (Information über angelegte/geänderte/gelöschte Datensätze)
Vom den Nutzern erzeugte Inhalte und Einstellungen	• persönliche Einstellungen, Angaben in Nutzerprofil, gespeicherte Inhalte in E-Mail, Chats, Kalendereinträge, Kommentare, Datenbankeinträge, Daten der unterrichteten bzw. verwalteten Schüler • Weitere Faktoren zur Anmeldung mittels Multi-Faktor-Authentifizierung (Telefon oder private E-Mail oder App oder Fragen)
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)

	Empfänger	Zweck	Daten
Intern	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
Extern	Alle Empfänger von E-Mails	Kommunikation	Anzeigename, E-Mailadresse
	Ireland Operations Limited, Carmanhall Road, Sandyford Industrial Estate, Dublin 18, Irland	Dienstbereitstellung, Service und Support	• 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 http://aka.ms/Wkcowi, der die EU Standardvertragsklauseln enthält. • Anmeldedaten: Speicherung in allen Microsoft-Anmeldeservern

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 Unterauftragnehmer 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 versperrt.
	Zugangskontrolle	Das Schulnetzwerk ist durch eine Firewall geschützt. Betriebssysteme der Verwaltungsmitarbeiter und Systembetreuer sind Windows 10 und durch Applikations- und Makro-Kontrolle geschützt.
	Zugriffskontrolle	Die Benutzerkonten der Verwaltungsmitarbeiter und Systembetreuer sind durch Multi-Faktor-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.