Kanton Zürich
Bildungsdirektion
Mittelschul- und Berufsbildungsamt
Digital Service Center Sek II

Kontakt: Mittelschul- und Berufsbildungsamt, Digital Service Center Sek II, Ausstellungsstrasse 80, 8090 Zürich
Telefon 043 259 77 27

Schulungsunterlagen IKT-Grundversorgung Sek II

Merkblatt (Vorgaben) Datenschutz und Informationsklassifizierung

Inhalt

Definitionen

Klassifikationsstufen und Unterschiede von Daten

Stufe	Beschreibung gemäss Besondere Informationssicherheits-richtlinie BISR 3 Richtlinie für Informationsklassifikation und -handhabung
Öffentlich	Informationen, die frei verfügbar und für die Öffentlichkeit ohne Einschränkungen zugänglich sind.
Intern	Informationen, die von Mitarbeitenden, Partnern oder Kunden erstellt oder im gegenseitigen Einverständnis der Bildungsdirektion zur Verfügung gestellt werden und deren unbefugte Weitergabe die Reputation oder das Vertrauen in die Bildungsdirektion verletzt.
Vertraulich	Informationen, die nur für einen definierten Personenkreis zugänglich sein sollen und/oder durch deren Bekanntmachung (auch innerhalb der kantonalen Verwaltung) ein wesentlicher Schaden verursacht werden könnte.
Geheim	Informationen werden als «Geheim» klassifiziert, wenn Unberechtigte durch deren Kenntnisnahme den Interessen des Kantons Zürich einen schweren Schaden zufügen könnten. Dazu gehören streng vertrauliche oder staatlich regulierte Informationen, deren Schutz und Geheimhaltung gesetzlich vorgeschrieben ist.

Daten	Beschreibung
Sachdaten	Informationen, die sich nicht auf Personen beziehen.
Personendaten	Informationen, die sich auf eine bestimmte oder auch nur bestimmbare natürliche oder juristische Person beziehen. Klassifizierung «**intern**» nach § 3 Abs.3 IDG (Gesetz über die Information und den Datenschutz)
Besondere Personendaten	Informationen, die folgende Eigenschaften aufweisen, z.B. • «Persönlichkeitsprofile», • religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, • Gesundheit, Intimsphäre, Rassenzugehörigkeit oder ethnische Herkunft, • administrative oder strafrechtliche Verfolgungen oder Sanktionen. Klassifizierung «**vertraulich**» nach § 3 Abs.4 IDG Angaben über Einkommens- und Vermögensverhältnisse fallen nicht unter den Begriff.

Beispiele je Klassifizierungsstufe

	Öffentlich	Intern	Vertraulich	Geheim
Folgen der Veröffentlichung	keine nachteiligen Auswirkungen	• geringer Reputationsverlust • geringer Vertrauensverlust • keine weitreichenden Konsequenzen	• mittlerer bis hoher Schaden (Reputationsverlust, erheblicher finanzieller Verlust), • rechtliche Konsequenzen (Ordnungswidrigkeiten, Geldstrafen)	• hoher bis sehr hoher Schaden • erheblicher Verlust von Reputation und Vertrauen in der Bevölkerung • Gravierende rechtliche Konsequenzen bis hin zu Haftstrafen • sehr schwerer finanzieller Verlust
Beispiele	• Informationsbroschüren • Informationen, die bereits publiziert sind, z.B. Jahresbericht • Bereits veröffentlichte Medienmitteilungen	• Arbeitsanweisungen • Prozessbeschreibungen, Abläufe • Richtlinien, Weisungen, Handbücher, Wegleitungen • Vorlagen intern (leer) • Interne Newsletter • Allgemeine E-Mails (ohne besondere Personendaten) • Kontaktdaten	• Schutzkonzepte, ISDS-Konzepte • Risikoanalysen • Personalbefragungen • Feedbackbögen • Zeiterfassungsdaten • Lohndaten • Gesundheitsdaten, Case-Management-Dossiers • Stellenplan	• Zugriffsinformationen, z.B. Passwörter, PIN • Kryptographische Schlüssel

	Öffentlich	Intern	Vertraulich	Geheim
		• Medienmitteilungen vor Veröffentlichung • Nutzungs- und Randdaten (Logfiles)	• Konfigurationsdaten (von Systemen) • Log-Daten (Protokollierung in Systemen) • Systemarchitektur • Kontodaten	
Schulbeispiele	• Webseiteninhalte • Stundenpläne • Broschüren • Plakate und weitere, veröffentlichte Informationen	• Schulmitteilungen • Intranet • Lehrmittel • Vorlagen • Unterrichtsfolien • Anleitungen • Adresslisten • Fotos (soweit nicht zur Veröffentlichung vorgesehen und Einverständniserklärung vorhanden), etc.	• Zeugnisse • einzelne Noten • Lernprofile • Disziplinarmassnahmen • Angaben über die Gesundheit wie auch Quarantänemassnahmen • Religionszugehörigkeit • Massnahmen zum Nachteilsausgleich (NAM), etc. • Dokumente für einen bestimmten Personenkreis (Beispiel Rektorat)	• Arztzeugnisse, Diagnosen (die zu NAM) führen • Korrespondenz zum Nachteilsausgleich (Diagnosen) • Hochsensible Informationen über Lernende, Bspw. strafrechtliche Sanktionen, • ärztliche Gutachten
Umgang allgemein	• Öffentliche Informationen können ohne Nachfrage weitergegeben werden.	• Informationen, die nur für die interne Verwendung bestimmt sind, können ohne Einschränkung an Mitarbeitende oder an andere öffentliche Stellen übermittelt werden, sofern dienstlich benötigt • Einschränkungen können sich ergeben, wenn die Information nicht für die Tätigkeit benötigt wird (Need-to-Know-Prinzip) • dürfen externen Beauftragten bei Vorliegen einer Geheimhaltungsverpflichtung zugänglich gemacht werden	• Informationen können einem bestimmten Personenkreis übermittelt werden, sofern dienstlich benötigt (bspw. einer Abteilung, Team oder Gruppe aufgrund ihrer Aufgabe) • dürfen externen Beauftragten nur mit Genehmigung des Dateneigentümers und bei Vorliegen einer Geheimhaltungsverpflichtung zugänglich gemacht werden	• Informationen dürfen nur an namentlich benannte Empfänger übermittelt werden • Informationen dürfen von jedem Empfänger nur mit Genehmigung des Dateneigentümers an andere Empfänger weitergeleitet werden. • Dürfen externen Beauftragten nur mit Genehmigung des Dateneigentümers und bei Vorliegen einer Geheimhaltungsverpflichtung zugänglich gemacht werden.

Verhalten jedes Einzelnen

- Beim Erstellen eines Dokumentes überlegen, welcher Schutzstufe (öffentlich, intern, vertraulich, geheim) der Inhalt zugeordnet werden kann.
- Es gilt der Grundsatz, je vertraulicher bzw. sensibler eine Information ist, desto stärker muss der Kreis der Personen, die die Information einsehen können, eingeschränkt werden. Dies bedeutet im M365- / Sharepoint-Umfeld, dass vertrauliche Informationen in Ablagen (Kanäle, Verzeichnisse) gespeichert werden müssen, auf die nur bestimmte Personen Zugriff haben.
- Daten, die in M365 gespeichert und innerhalb der Schule weitergegeben werden, sind bereits durch M365 verschlüsselt. Sobald die Informationen die Schule z.B. per E-Mail verlassen, muss beachtet werden, dass E-Mails mit vertraulichem Inhalt oder Anhang zusätzlich verschlüsselt sind. Siehe dazu das DSC-Merkblatt zur Mailverschlüsselung. Auch beim Freigeben / Teilen von Dateien ist das zu beachten.
- Vorsicht beim Teilen des Bildschirms, z.B. mit Supportstellen oder anderen Ämtern. Es dürfen keine vertraulichen Informationen gezeigt werden.
- Beim Verlassen des Arbeitsplatzes immer den Bildschirm sperren, auch wenn der Platz für weniger als eine Minute verlassen wird.
- Starke Passwörter verwenden. Unter www.passwortcheck.ch kann das Passwort überprüft werden (bitte ein ähnliches Passwort eingeben).
- Keine vertraulichen oder geheimen Dokumente auf dem Pult (auch im Homeoffice), noch beim Drucker liegen lassen.