Seite 5.2 Verantwortungsbewusster Umgang mit digitalen Medien

Prüfungsziel

Du sollst erklären können, wie man digitale Medien im Betrieb verantwortungsvoll nutzt und dabei Persönlichkeitsrechte, Datenschutz und die Wirkung des eigenen Kommunikationsverhaltens beachtet.

Für die Prüfung sind hier vor allem wichtig:

- verantwortungsvoller Umgang mit digitalen Medien
- Zusammenarbeit im virtuellen Raum
- Wahrung der Persönlichkeitsrechte Dritter
- Speicherung digitaler Inhalte
- Darstellung digitaler Inhalte
- Weitergabe digitaler Inhalte
- Auswirkungen des eigenen Kommunikationsverhaltens
- Auswirkungen des eigenen Informationsverhaltens
- respektvolle digitale Kommunikation
- bewusster Umgang mit Informationen

Was sind digitale Medien?

Digitale Medien sind elektronische Medien, mit denen Informationen erstellt, gespeichert, übertragen oder ausgetauscht werden.

Beispiele:

- E-Mail
- Chat
- Ticketsystem
- Videokonferenz
- Cloudspeicher
- Messenger
- Intranet
- Wiki
- Lernplattform
- Social Media
- Projektmanagement-Tools
- digitale Dokumente
- Screenshots
- Fotos
- Videos

- geteilte Kalender

Was bedeutet verantwortungsvoller Umgang mit digitalen Medien?

Verantwortungsvoller Umgang bedeutet, digitale Medien bewusst, sicher, respektvoll und rechtlich korrekt zu nutzen.

Einfach gesagt:

Nicht alles, was technisch möglich ist, ist auch erlaubt oder sinnvoll.

Man muss beachten:

- Welche Informationen teile ich?
- Mit wem teile ich sie?
- Darf ich diese Information weitergeben?
- Sind personenbezogene Daten enthalten?
- Könnte jemand dadurch geschädigt werden?
- Ist der Ton respektvoll?
- Ist der Empfängerkreis richtig?
- Ist die Information vertraulich?
- Ist die Quelle zuverlässig?

Warum ist das im Betrieb wichtig?

Digitale Kommunikation ist schnell, aber Fehler verbreiten sich ebenfalls schnell.

Mögliche Risiken:

- vertrauliche Daten werden an falsche Personen gesendet
- personenbezogene Daten werden unzulässig geteilt
- Missverständnisse durch unklare Nachrichten
- Imageschaden durch unbedachte Äußerungen
- Konflikte durch unhöfliche Kommunikation
- Datenschutzverstöße
- Sicherheitsrisiken
- falsche Informationen verbreiten sich
- Persönlichkeitsrechte werden verletzt

Persönlichkeitsrechte Dritter

Persönlichkeitsrechte schützen die Würde, Privatsphäre und persönliche Entfaltung von Menschen.

Im Betrieb bedeutet das:

Man darf andere Personen nicht ohne Grund bloßstellen, überwachen, beleidigen, fotografieren, filmen oder personenbezogene Informationen verbreiten.

Beispiele für geschützte Informationen:

- Name
- Adresse
- Telefonnummer
- E-Mail-Adresse
- Geburtsdatum
- Foto
- Video
- Gesundheitsdaten
- Leistungsdaten
- Personalakte
- private Nachrichten
- Standortdaten
- Bewertungen über eine Person

Beispiele für Verletzungen von Persönlichkeitsrechten

Situation	Problem
Foto eines Kollegen ohne Zustimmung im Intranet hochladen	Recht am eigenen Bild verletzt
Screenshot mit Kundendaten im Chat teilen	Datenschutzproblem
private Information über Kollegen weiterleiten	Verletzung der Privatsphäre
abwertender Kommentar über Mitarbeiter im Gruppenchat	respektlos und möglicherweise rechtlich problematisch
ungefragtes Aufzeichnen einer Videokonferenz	Persönlichkeitsrechte und Datenschutz betroffen
Leistungsdaten öffentlich im Team posten	Bloßstellung und Datenschutzrisiko

---

Recht am eigenen Bild

Das Recht am eigenen Bild bedeutet, dass Menschen grundsätzlich selbst entscheiden dürfen, ob Bilder von ihnen veröffentlicht oder verbreitet werden.

Prüfungsnah:

Ein Foto von Kollegen, Kunden oder Besuchern sollte nicht einfach ohne Zustimmung veröffentlicht oder weitergegeben werden.

Beispiel:

Ein Azubi macht ein Foto vom Team und lädt es ohne Nachfrage in eine öffentliche Social-Media-Gruppe hoch.

Das ist problematisch, weil die abgebildeten Personen nicht zugestimmt haben.

Speichern digitaler Inhalte

Beim Speichern digitaler Inhalte muss geprüft werden, ob die Speicherung notwendig, erlaubt und sicher ist.

Beispiele für digitale Inhalte:

- Kundendaten
- Mitarbeiterdaten
- Tickets
- Chatverläufe
- E-Mails
- Screenshots
- Logs
- Fotos
- Dokumente
- Vertragsdaten
- Projektdaten

Wichtige Fragen:

- Darf ich diese Daten speichern?
- Gibt es einen betrieblichen Zweck?
- Sind personenbezogene Daten enthalten?
- Wo werden die Daten gespeichert?
- Wer hat Zugriff?
- Wie lange werden die Daten benötigt?
- Müssen Daten gelöscht werden?
- Ist die Speicherung sicher?

Darstellung digitaler Inhalte

Darstellung bedeutet, wie Inhalte angezeigt oder präsentiert werden.

Beispiele:

- Bildschirmfreigabe in Videokonferenz
- Präsentation
- Dashboard
- Monitoring-Anzeige

- Ticketübersicht
- Chatnachricht
- Screenshot
- Wiki-Seite
- Intranet-Beitrag

Risiken bei der Darstellung:

- vertrauliche Daten sind sichtbar
- falsche Personen sehen Kundendaten
- private Nachrichten werden versehentlich gezeigt
- Passwörter oder Tokens sind sichtbar
- personenbezogene Daten werden unnötig angezeigt
- sensible Tickets werden im Meeting geteilt

Beispiel: Bildschirmfreigabe

Ein Mitarbeiter teilt in einer Videokonferenz seinen Bildschirm.

Auf dem Desktop sind sichtbar:

- private E-Mails
- Kundendaten
- interne Tickets
- Zugangsdaten in einer Datei
- Chatnachrichten

Richtiges Verhalten:

- nur das benötigte Fenster teilen
- sensible Tabs schließen
- Benachrichtigungen deaktivieren
- keine Passwörter sichtbar lassen
- vor der Freigabe prüfen, was zu sehen ist

Weitergabe digitaler Inhalte

Weitergabe bedeutet, dass Informationen an andere Personen oder Stellen übermittelt werden.

Beispiele:

- E-Mail weiterleiten
- Datei in Cloud teilen
- Screenshot senden
- Link freigeben

- Chatnachricht kopieren
- Dokument exportieren
- Daten an Dienstleister senden
- Logdatei an Support weitergeben

Wichtige Fragen vor der Weitergabe:

- Ist die Weitergabe erlaubt?
- Ist der Empfänger berechtigt?
- Sind personenbezogene Daten enthalten?
- Ist die Datei wirklich notwendig?
- Müssen Daten anonymisiert werden?
- Ist der Übertragungsweg sicher?
- Ist der Empfängerkreis zu groß?
- Gibt es vertrauliche Informationen?

Empfängerkreis prüfen

Ein häufiger Fehler ist, Informationen an zu viele oder falsche Personen zu senden.

Beispiele:

Fehler	Risiko
„Allen antworten“ ohne Prüfung	zu viele Personen erhalten Informationen
falsche E-Mail-Adresse	Daten gehen an falschen Empfänger
offene Verteilerliste	E-Mail-Adressen werden sichtbar
Cloud-Link öffentlich freigegeben	unberechtigte Personen können zugreifen
Screenshot in Gruppenchat	sensible Informationen erreichen falsche Personen

---

Kommunikationsverhalten

Kommunikationsverhalten beschreibt, wie jemand Informationen austauscht.

Gutes Kommunikationsverhalten ist:

- sachlich
- höflich
- verständlich
- zielgerichtet
- respektvoll
- vollständig genug
- nicht unnötig lang
- empfängerorientiert

- datenschutzbewusst
- sicherheitsbewusst

Schlechtes Kommunikationsverhalten

Schlechtes Kommunikationsverhalten kann Konflikte oder Schäden verursachen.

Beispiele:

- unhöfliche Nachrichten
- unklare Anweisungen
- Schuldzuweisungen im Chat
- vertrauliche Informationen in offenen Kanälen
- unnötig viele Personen in CC
- private Kritik in öffentlicher Gruppe
- Weiterleitung ohne Prüfung
- vorschnelles Teilen unbestätigter Informationen
- Screenshots mit sichtbaren Kundendaten

Informationsverhalten

Informationsverhalten beschreibt, wie jemand Informationen sucht, bewertet, speichert, nutzt und weitergibt.

Gutes Informationsverhalten bedeutet:

- Quellen prüfen
- Informationen nicht ungeprüft weitergeben
- vertrauliche Informationen schützen
- nur notwendige Daten speichern
- Informationen aktuell halten
- klare Ablage nutzen
- Daten nicht unnötig vervielfältigen
- falsche Informationen korrigieren
- Berechtigungen beachten

Beispiel: Falsche Information im Betrieb

Ein Mitarbeiter liest in einem Chat, dass ein System angeblich ausgefallen ist.

Er informiert sofort mehrere Kunden, ohne die Information zu prüfen.

Später stellt sich heraus, dass es nur ein lokales Problem war.

Problem:

- unnötige Unruhe
- Vertrauensverlust
- zusätzliche Arbeit
- falsche Kommunikation
- schlechter Eindruck beim Kunden

Richtiges Verhalten:

Erst prüfen, dann gezielt informieren.

Zusammenarbeit im virtuellen Raum

Virtueller Raum bedeutet digitale Zusammenarbeit ohne gemeinsamen physischen Ort.

Beispiele:

- Videokonferenz
- Chat
- Cloud-Dokument
- Ticketsystem
- Remote-Support
- Online-Schulung
- gemeinsames Wiki
- Projektmanagement-Tool

Regeln für gute virtuelle Zusammenarbeit

- pünktlich an Meetings teilnehmen
- Mikrofon stummschalten, wenn man nicht spricht
- andere ausreden lassen
- klare Beiträge schreiben
- Aufgaben dokumentieren
- Zuständigkeiten festhalten
- Entscheidungen nachvollziehbar speichern
- vertrauliche Informationen schützen
- passende Kanäle nutzen
- nicht in zu vielen parallelen Chats arbeiten
- Datenschutz beachten

Digitale Inhalte und Dauerhaftigkeit

Digitale Inhalte können lange gespeichert, kopiert und weitergeleitet werden.

Wichtig:

Was einmal digital geteilt wurde, lässt sich oft schwer vollständig zurückholen.

Beispiele:

- weitergeleitete Screenshots
- exportierte Chatverläufe
- heruntergeladene Dateien
- E-Mail-Anhänge
- öffentliche Social-Media-Beiträge
- geteilte Cloud-Links

Prüfungsnah:

Vor dem Teilen überlegen, ob Inhalt, Empfänger und Zweck passen.

Umgang mit Screenshots

Screenshots sind im IT-Bereich nützlich, aber riskant.

Nützlich für:

- Fehlermeldungen
- Dokumentation
- Supportfälle
- Schulungsunterlagen
- Beweise für Systemzustände

Risiken:

- Kundendaten sichtbar
- personenbezogene Daten sichtbar
- interne Systeme sichtbar
- IP-Adressen oder Hostnamen sichtbar
- Zugangsdaten sichtbar
- vertrauliche Tickets sichtbar

Richtiges Verhalten:

- sensible Daten schwärzen
- nur nötigen Bildausschnitt verwenden
- Empfänger prüfen
- Screenshot sicher speichern
- Screenshot löschen, wenn nicht mehr benötigt

Umgang mit Links und Freigaben

Cloud-Links und Datei-Freigaben müssen vorsichtig genutzt werden.

Risiken:

- Link ist öffentlich erreichbar
- falsche Berechtigung
- Bearbeitungsrechte statt Leserechte
- Link wird weitergeleitet
- Ablaufdatum fehlt
- Datei enthält sensible Daten

Sichere Maßnahmen:

- Empfänger gezielt festlegen
- nur notwendige Rechte vergeben
- Ablaufdatum setzen, wenn möglich
- Passwortschutz nutzen, wenn sinnvoll
- Freigaben regelmäßig prüfen
- öffentliche Links vermeiden, wenn vertrauliche Daten enthalten sind

---

Umgang mit Kundendaten

Kundendaten sind besonders schützenswert.

Grundregeln:

- nur für dienstliche Zwecke nutzen
- nicht privat speichern
- nicht an Unbefugte weitergeben
- nicht in unsicheren Chats teilen
- nicht in privaten Cloudspeichern ablegen
- nur notwendige Daten verwenden
- Zugriffsrechte beachten
- Daten löschen, wenn sie nicht mehr benötigt werden und keine Aufbewahrungspflicht besteht

---

Bezug zur IT-Sicherheit

Verantwortungsvoller Umgang mit digitalen Medien hat auch mit IT-Sicherheit zu tun.

Beispiele:

- keine vertraulichen Informationen in unsicheren Kanälen
- keine Passwörter per Klartext senden
- keine unbekannten Links öffnen

- keine sensiblen Anhänge an falsche Empfänger
- Vorsicht bei Phishing
- Berechtigungen prüfen
- sichere Kommunikationswege nutzen

Bezug zur Prüfung

In der Prüfung können Situationen beschrieben werden, bei denen du richtiges oder falsches Verhalten im Umgang mit digitalen Medien erkennen sollst.

Typische Aufgaben:

- Persönlichkeitsrechte erkennen
- unzulässige Weitergabe von Informationen beurteilen
- richtige digitale Kommunikationsweise auswählen
- falsche Adressatenlisten erkennen
- Screenshot-Risiken bewerten
- Cloud-Freigaben beurteilen
- Datenschutz und Kommunikation zusammen betrachten
- Auswirkungen des eigenen Informationsverhaltens erklären

Typische Prüfungsfrage 1

Was bedeutet verantwortungsvoller Umgang mit digitalen Medien?

Antwort anzeigen

Verantwortungsvoller Umgang mit digitalen Medien bedeutet, digitale Medien bewusst, sicher, respektvoll und rechtlich korrekt zu nutzen.

Typische Prüfungsfrage 2

Warum sind Persönlichkeitsrechte bei digitaler Zusammenarbeit wichtig?

Antwort anzeigen

Persönlichkeitsrechte schützen die Privatsphäre, Würde und persönlichen Daten von Menschen. Digitale Inhalte wie Fotos, Screenshots oder personenbezogene Informationen dürfen nicht unbedacht gespeichert oder weitergegeben werden.

Typische Prüfungsfrage 3

Nenne drei Beispiele für digitale Medien im Betrieb.

Antwort anzeigen

Beispiele sind E-Mail, Chat, Ticketsystem, Videokonferenz, Cloudspeicher, Intranet, Wiki, Messenger und Projektmanagement-Tools.

Typische Prüfungsfrage 4

Warum ist ein Screenshot im Supportfall manchmal riskant?

Antwort anzeigen

Ein Screenshot kann Kundendaten, personenbezogene Daten, interne Systeme, Zugangsdaten oder vertrauliche Informationen sichtbar machen.

Typische Prüfungsfrage 5

Was sollte man vor der Weitergabe digitaler Inhalte prüfen?

Antwort anzeigen

Man sollte prüfen, ob die Weitergabe erlaubt ist, ob der Empfänger berechtigt ist, ob personenbezogene oder vertrauliche Daten enthalten sind und ob der Übertragungsweg sicher ist.

Typische Prüfungsfrage 6

Warum ist „Allen antworten“ bei E-Mails manchmal problematisch?

Antwort anzeigen

Weil dadurch Informationen an Personen gelangen können, die diese nicht benötigen oder nicht erhalten dürfen. Das kann Datenschutz- oder Vertraulichkeitsprobleme verursachen.

Typische Prüfungsfrage 7

Was ist gutes Kommunikationsverhalten in digitalen Medien?

Antwort anzeigen

Gutes Kommunikationsverhalten ist sachlich, höflich, verständlich, zielgerichtet, respektvoll, empfängerorientiert, datenschutzbewusst und sicherheitsbewusst.

Typische Prüfungsfrage 8

Was bedeutet gutes Informationsverhalten?

Antwort anzeigen

Gutes Informationsverhalten bedeutet, Informationen zu prüfen, vertrauliche Daten zu schützen, nur notwendige Daten zu speichern, Berechtigungen zu beachten und Informationen nicht ungeprüft weiterzugeben.

Typische Prüfungsfrage 9

Warum sollte man Cloud-Freigaben regelmäßig prüfen?

Antwort anzeigen

Weil Freigaben sonst zu lange bestehen bleiben, falsche Personen Zugriff haben können oder vertrauliche Daten unberechtigt erreichbar sind.

Typische Prüfungsfrage 10

Warum sollte man digitale Inhalte vor dem Teilen sorgfältig prüfen?

Antwort anzeigen

Digitale Inhalte können schnell kopiert, weitergeleitet und lange gespeichert werden. Fehlerhafte oder vertrauliche Inhalte lassen sich oft schwer zurückholen.

Merksatz

- Digitale Medien müssen bewusst, sicher und respektvoll genutzt werden
- Persönlichkeitsrechte schützen Privatsphäre, Würde und persönliche Daten
- Nicht alles, was technisch möglich ist, ist erlaubt oder sinnvoll

- Vor dem Speichern, Darstellen und Weitergeben digitaler Inhalte immer Zweck, Empfänger und Inhalt prüfen
- Screenshots können sensible Daten enthalten
- Cloud-Freigaben und Links müssen gezielt und begrenzt vergeben werden
- Gute digitale Kommunikation ist sachlich, höflich, klar und datenschutzbewusst
- Gutes Informationsverhalten bedeutet: prüfen, schützen, gezielt weitergeben

---

Revision #1
Created 26 May 2026 12:59:09 by Admin
Updated 26 May 2026 13:47:57 by Admin