Anlage 5 - Nutzungsmöglichkeiten und Zweckbindungen von Programmen, Apps und Diensten

Präambel

Die BBS Meppen stellen allen Mitgliedern der Schulgemeinschaft (im Folgenden: Nutzerinnen und Nutzer) neben der schulischen Plattform „IServ“ und einem individuellen WLAN-Zugang verschiedene Programme und Apps bereit, die mit schuleigenen und privaten Endgeräten (z. B. Notebooks, Tablets und Smartphones) ausschließlich für schulische Zwecke, also um schulbezogene Daten zu speichern und auszutauschen, genutzt werden kann, zur Verfügung.

Nutzungsmöglichkeiten und Zeckbindung

Die von den BBS Meppen zur Verfügung gestellten Programme, Apps und Dienste sind ausschließlich für schulische und bildungsbezogene Zwecke bestimmt. Dies gilt sowohl für die Nutzung in der Schule als auch zu Hause. Die Verwendung für private, gewerbliche oder kommerzielle Zwecke ist nicht gestattet. Insbesondere ist es untersagt:

- mit der bereitgestellten Software erstellte Inhalte oder Ergebnisse kommerziell zu nutzen oder zu verwerten,
- die Software für die Erstellung von Produkten oder Dienstleistungen zu verwenden, die verkauft oder anderweitig wirtschaftlich verwertet werden sollen,
- die Lizenzen, Programme oder Zugangsdaten an Dritte weiterzugeben oder
- die Software für außerschulische Projekte oder Aufträge zu nutzen.
  Bei Unsicherheit über die zulässige Nutzung ist vorab die Genehmigung der Schulleitung einzuholen.

Verhaltensregeln

Alle Nutzerinnen und Nutzer verpflichten sich, die Rechte anderer Personen zu achten. Dies betrifft nicht nur den Datenschutz, sondern auch Persönlichkeitsrechte im Rahmen des Urheber- und Medienrechts sowie des Jugendschutzes.
Darüber hinaus verpflichten sich alle Nutzerinnen und Nutzer, digitale Werkzeuge kritisch und reflektiert zur Aneignung und Vertiefung fachlicher Inhalte einzusetzen und digitale Medien zur Förderung ihrer fachlichen Kompetenzen verantwortungsvoll zu nutzen.
Bei der Nutzung von sämtlichen Digitalgeräten, insb. von Smartwatches ist die Mithörfunktion grundsätzlich zu deaktivieren; eine Nutzung zur Überwachung von Gesprächen oder Unterrichtsgeschehen ist strikt untersagt.
Die Mitglieder der Schulgemeinschaft erhalten, sofern benötigt, individuelle Zugangsdaten und ein ggf. vorläufiges Passwort. Dieses ist umgehend nach Erhalt oder bei Verdacht auf Kenntnisnahme durch Dritte durch ein individuelles 8-stelliges Passwort zu ersetzen. Darin müssen mindestens drei der vier Elemente Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen enthalten sein. Die Verantwortlichkeit für Vorgänge auf dem Nutzerkonto liegt immer bei dem Inhaber dieses Kontos.
Von der Möglichkeit, im Nutzerprofil persönliche Daten einzugeben, sollte kein Gebrauch gemacht werden, da eingegebene Daten für alle Nutzerinnen und Nutzer sichtbar sind.

Alle Nutzerinnen und Nutzer verpflichten sich, die gesetzlichen Regelungen des Strafrechtes und Jugendschutzes sowie des Urheberrechtes zu beachten. Wer Dateien über die im Rahmen der bereit gestellten Programme, Apps und Dienste hochlädt, versendet oder nutzt, übernimmt damit die Verantwortung. Die Schule übernimmt keine Verantwortung für die Inhalte und die Art sämtlicher gespeicherter Daten, hat aber in begründeten Fällen die Möglichkeit, diese Daten einzusehen. Auch das Aufrufen und Speichern jugendgefährdender und anderer strafrechtlich relevanter Inhalte auf den Schulserver ist verboten, das gilt auch für die Speicherung von entsprechenden URLs (Webseiten) oder Links. Die gesetzlichen Bestimmungen insbesondere des Strafrechts, Urheberrechts und des Jugendschutzrechts sind zu beachten: Es ist verboten, pornografische, gewaltverherrlichende oder rassistische Inhalte aufzurufen, zu speichern oder zu versenden. Diskriminierungen, persönliche Angriffe, Unterstellungen und Verleumdungen sind untersagt und

können neben dem Entzug der Nutzungsberechtigung und sonstigen schulordnungsrechtlichen Maßnahmen auch zu einer zivil- oder strafrechtlichen Verfolgung führen. Zudem wird von allen Nutzerinnen und Nutzern erwartet, ihr eigenes Medienhandeln regelmäßig zu reflektieren, um einen bewussten, verantwortungsvollen und entwicklungsförderlichen Umgang mit digitalen Medien sicherzustellen.

Die Sicherung aller gespeicherten persönlichen Daten in den verschiedensten angebotenen Programmen, Apps und Diensten liegt ausschließlich in der Verantwortung der Nutzerinnen bzw. Nutzer, für einen möglichen Verlust haftet die Schule nicht.

Durch Lehrkräfte digital bereitgestelltes Material ist nur zur persönlichen Verwendung durch Schülerinnen und Schüler vorgesehen. Eine Weitergabe an Dritte außerhalb der Schulgemeinschaft, die Veröffentlichungen über Internetdienste oder in gedruckter Form ist nicht gestattet. Hausaufgaben können über die Kommunikationsplattform IServ gestellt werden, werden aber in der Regel im Unterricht angekündigt.

Die vorgegebene Ordnerstruktur in bestimmten Gruppen (Lehrer, Bildungsgangs- und Fachgruppen) darf in der ersten Ebene nicht verändert werden.

Das „IServ"-System erstellt automatische Protokolle (Log-Dateien), die in begründeten Fällen (Verstöße gegen rechtliche oder schulische Regeln) durch von der Schulleitung bestimmte Personen ausgewertet werden können. Im Missbrauchsfalle kann die Schulleitung diese Log-Dateien mit Angabe der persönlichen Daten an die zuständigen Strafverfolgungsbehörden (Polizei oder Staatsanwaltschaft) weitergeben.

Alle Nutzerinnen und Nutzer sind verpflichtet, eingesetzte Filter und Sperren zu respektieren und diese nicht zu umgehen. Solche oder ähnliche Manipulationsversuche an der Kommunikationsplattform werden zur Anzeige gebracht.

Die schulische Geräteausstattung darf nicht dazu genutzt werden, Vertragsverhältnisse einzugehen oder kostenpflichtige Dienste im Internet zu nutzen.

Passwortverlust

Schülerinnen und Schüler setzen im Falle des Passwortverlustes ihr Passwort selbstständig zurück oder wenden sich an die jeweils zuständige Lehrkraft. Neu vergebene Passwörter sind unverzüglich gemäß der bekannten Passwortregeln zu ändern.

Für eine reibungslose nächtliche Software- und Updateinstallation ist es erforderlich, dass die Arbeitsstationen am Ende des Schultages nicht von der Spannungsversorgung getrennt, jedoch trotzdem heruntergefahren werden.

Nutzung der Plattformen mit privaten Endgeräten per WLAN

Die Nutzung der schulischen Kommunikationsplattform „IServ" durch private Endgeräte ist in der Schule möglich. Dieser Zugang erfolgt mit den individuellen Zugangsdaten, ist also personenbezogen. Auch bei gutgläubiger, aber unerlaubter Weitergabe dieser Zugangsdaten an Dritte haftet immer die registrierte Nutzerin bzw. der registrierte Nutzer für unzulässige Aktivitäten.

Die BBS Meppen und der Landkreis Emsland als Schulträger übernehmen keine Haftung für die Datensicherheit und die physische Unversehrtheit privater Endgeräte in versicherungstechnischer Hinsicht.

Auch die WLAN-Nutzung wird automatisch in Log-Dateien protokolliert. Dazu gehört bspw. die IP-Adresse des Endgeräts, von dem aus auf das Internet zugegriffen wird, Datum und Uhrzeit des Internetzugriffs, die URL der aufgerufenen Seite, das Modell und die Version des Endgeräts oder die MAC-Adresse. In begründeten Fällen, z. B. bei Rechtsverstößen, können diese Protokolle durch die von der Schulleitung bestimmten Personen ausgewertet werden. Darüber hinaus kann die Schulleitung im Missbrauchsfalle diese Log-Dateien zusammen mit den persönlichen Nutzerdaten an Strafverfolgungsbehörden (Polizei und Staatsanwaltschaft) weitergeben.

E-Mail, Chats, Videokonferenzen und weitere Kommunikationskanäle der Plattform „IServ“

Das durch die BBS Meppen mit Einrichtung des Nutzerkontos zur Verfügung gestellte E-Mail-Konto ist aus- schließlich für schulische Kommunikation (interner Gebrauch) zu verwenden.

Die BBS Meppen sind damit **kein Anbieter von Telekommunikationsdienstleistungen** im Sinne des Telekommunikationsgesetzes.
Die Schulleitung oder eine von ihr beauftragte Person ist berechtigt, bei Verdacht auf missbräuchliche oder strafrechtlich relevante Nutzung, die Inhalte der Kommunikation zur Kenntnis zu nehmen. Die betroffene Nutzerin bzw. der betroffene Nutzer werden hierüber unverzüglich informiert. Wer Kenntnis von missbräuchlicher Nutzung der Kommunikationsplattform erhält (z. B. in Fällen von Cybermobbing, Verbreitung jugendgefährdender oder extremistischer Inhalte), hat dieses unverzüglich der Schulleitung mitzuteilen.

Bei Videokonferenzen übernimmt die Lehrkraft die Rolle der Konferenzmoderation und stellt sicher, dass Personen, die unbefugt teilnehmen, erkannt und ausgeschlossen werden.
Schülerinnen und Schüler verlassen die Videokonferenz, wenn die Lehrkraft durch Fremdeinwirken von der Videokonferenz ausgeschlossen wurde oder fremde Personen unerwartet teilnehmen.

Verstöße

Im Fall von Verstößen gegen die Nutzungsordnung wird das Nutzerkonto gesperrt und ggfs. werden weitere Maßnahmen eingeleitet (vgl. Punkt 3.6 der Schulordnung).

Datenlöschung

Mit dem Austritt aus der Schulgemeinschaft werden das individuelle „IServ“-Konto sowie die von der Schule bereit gestellten Programme, Apps und Dienste (wie z. B. Office365, GoodNotes, Canva) inklusive aller ~~darauf~~ gespeicherten Daten gelöscht. Die Verantwortung für die rechtzeitige Sicherung liegt ausschließlich bei den Nutzerinnen und Nutzern. Nach der Löschung des Kontos ist keine Wiederherstellung der Daten möglich. Die Schule übernimmt keine Haftung für verlorene Daten.

Nutzung von KI-Tools:

Anwendung: Wenn die Lehrkraft es zulässt, dürfen KI-Werkzeuge sowohl im Unterricht als auch bei den Hausaufgaben, beim Generieren von Ideen und beim Verfassen von Texten genutzt werden. Auch die eigentliche Anwendung eines KI-Tools kann Gegenstand im Unterricht sein. Es kann auch Unterrichtsphasen oder Hausaufgaben geben, in denen die Nutzung von KI bewusst ausgeschlossen wird. Kommt ein KI-Tool verpflichtend zur Anwendung, stellt die Lehrkraft einen DSGVO-konformen Zugang für alle bereit. Es besteht keine Pflicht, einen privaten Zugang anzulegen. Die Ressourcen sind grundsätzlich effizient zu nutzen.

Verantwortung für das Ergebnis: Da alle Hilfsmittel ihre Grenzen haben, können die Suchergebnisse veraltet, falsch, ungenau oder mit Vorurteilen behaftet sein. Die Ergebnisse sind zu überprüfen und gegebenenfalls zu überarbeiten. Für fehlerhafte Lösungen sind ausschließlich die Nutzerinnen und Nutzer verantwortlich, nicht das Werkzeug.

Quellenhinweise: Alle unter Verwendung von KI-Tools erstellten Inhalte müssen eindeutig als solche gekennzeichnet werden. Dies gilt für alle schulischen Arbeiten, einschließlich Hausaufgaben, Präsentationen, Referate und sonstige Leistungen. Bei Hausaufgaben reicht der Name des Werkzeuges direkt am jeweiligen Lösungsschritt. Bei umfangreicheren Leistungen ist in bekannter Weise zu zitieren (vgl. Hinweise zur Zitiertechnik an den BBS Meppen).

Täuschungsversuch: Werden Inhalte, die mithilfe von KI-Tools erstellt oder überarbeitet wurden, nicht oder nicht ausreichend gekennzeichnet, wird dies in der Regel als Täuschungsversuch gewertet. Dies gilt insbesondere dann, wenn der Eindruck entsteht, die Leistung sei vollständig ohne den Einsatz von KI erbracht worden oder wenn der Umfang der KI-Nutzung nicht transparent offengelegt wird.

Bei der Bewertung kann die Schule ihre Entscheidung auf dokumentierte Anhaltspunkte stützen, beispielsweise auf eine deutliche Abweichung vom bisherigen Leistungsstand, unplausible Quellen-

oder Arbeitsnachweise oder Widersprüche in der mündlichen Erläuterung.

Datenschutz und Ethik: Bei der Nutzung einer KI sind die Datenschutzbestimmungen einzuhalten. Persönliche Daten oder Informationen anderer dürfen nicht ohne deren Einwilligung verarbeitet oder eingegeben werden. Außerdem ist es untersagt, die KI für unethische Zwecke, wie die Erstellung beleidigender, diskriminierender oder rechtswidriger Inhalte zu nutzen.

Für Prüfungssituationen gelten andere Regeln. Dort ist die KI nur dann zugelassen, wenn die Nutzung ausdrücklich erlaubt wurde.

Nutzung schuleigener Endgeräte (PCs, Notebooks, Tablet-PCs)

Schuleigene Endgeräte sind pfleglich zu behandeln, Schäden sind sofort einem Mitglied des Administratorenteams zu melden.

Die Installation oder Nutzung schulfremder Software durch die Nutzerinnen und Nutzer ist unzulässig. Soft- wareinstallationen werden auf Anfrage bzw. nach Prüfung auf Notwendigkeit kurzfristig durch ein Mitglied des Administratorenteams durchgeführt.

Bei Verlassen des PC-Arbeitsplatzes ist aus Datenschutzgründen darauf zu achten, sich vom Benutzerkonto abzumelden (Tastenkombination Alt + F4 und Enter-Taste) bzw. den PC zu sperren (Tastenkombination <Win> + <L>).

Nutzung der Arbeitsplätze in den PC-Räumen

Zusätzlich zu den bereits vorhandenen IT-Regelungen gilt für die EDV-Räume:

- Getränke dürfen nur mit einem Mindestabstand von einem Meter zum PC-Arbeitsplatz zu sich genommen werden.
- Die Lagerung von Getränken auf dem Tisch des PC-Arbeitsplatzes ist nicht zulässig.
- Druckaufträge sind nur nach Absprache mit der zuständigen Lehrkraft auszuführen.
- Die Hardware-Konfiguration darf nicht verändert werden, d. h., Eingriffe an der Hardware sind strikt untersagt.
- Die Nutzung mitgebrachter Datenträger (z .B. USB-Sticks) ist mit Zustimmung der Lehrkräfte gestattet. Private Hardware, z. B. Notebooks, dürfen nur im schuleigenen WLAN-Netz „BBS Meppen" betrieben werden.
- Die Verwendung fremder Software ohne Zustimmung der Lehrkraft ist strikt untersagt. Davon ausgenommen sind PC-Labore, in denen die Softwareinstallation Unterrichtsinhalt ist.

Die Stühle in den PC-Räumen dürfen nicht auf die Tische gestellt werden, diese werden an den Tisch herangeschoben.