

הנחיות לשימוש ב"סביבת ענן" במוסדות חינוך

מסמך זה מהווה הנחייה לשימוש ב"סביבת ענן" במוסדות החינוך בכל הקשור למחזור החיים של חשבון משתמש ולשימוש שוטף בדגש על היבטים של אבטחת מידע ושמירת הפרטיות.

הנחיות למוסדות החינוך לשמירה על אבטחת מידע ופרטיות ביישומי ענן:

1. מנהלי בית ספר הינם הגורם האחראי ליישום הנחיות אבטחת המידע ופרטיות בבתי הספר בסביבות יישומי ענן.
2. ניתן להשתמש אך ורק ברישוי המיועד לחינוך - Microsoft Office 365 Education, Google Workspace for Education.
3. בעת חיבור המוסד לסביבת ענן של המשרד, יש להגדיר מנהל לסביבה (Admin) מטעם בית הספר. מנהל הסביבה יכול להיות מנהל המוסד החינוכי, רכז התקשוב, מתאם המחשוב או גורם אחר מסגל בית הספר אותו ממנה המנהל אשר עבר הדרכה לנושא ואושר ע"י משרד החינוך.
4. על כלל מנהלי סביבות הענן להשתמש בהזדהות משרד החינוך / מנגנון הזדהות חזקה של סביבת הענן הכוללת סיסמה אישית חזקה ומנגנון לאימות רב שלבי (MFA-Multi Factor Authentication), כגון קבלת מסרון עם קוד לנייד או לדוא"ל. הנחיה זו מתייחסת גם לאדמיניסטרטורים חיצוניים לבית הספר (כגון עובדי ספק) שאושרו על ידי משרד החינוך.
5. יש לאפשר לחטיבת הסייבר במשרד החינוך גישה שוטפת לסביבת הענן לצורכי בקרה, תחקור וטיפול באירועי אבטחת מידע. במידת הצורך, ככל ויידרש ייפתח חשבון אדמין לנציג המשרד על פי דרישה.
6. ככלל, יש להקפיד על הכללים הבאים בעת העברת ושמירת מידע בסביבות הענן המאושרות:
 - 6.1. בעת העבודה השוטפת של בית הספר נעשה שימוש במידע אישי של עובדי הוראה, תלמידים והוריהם, אשר חשיפתו עלולה לגרום לדלף מידע ולעבירה על חוק הגנת הפרטיות. על כן, יש להקפיד על שמירת המידע במקומות ייעודים ומאושרים שהוגדרו לצורך זה.
 - 6.2. חל איסור מוחלט להעביר מידע אישי (כגון: ת.ז, שם מלא, כתובת, כתובת מייל, מספר טלפון, מידע רפואי/פסיכולוגי וכו'). באמצעות חשבונות ענן פרטיים (כגון Gmail פרטי).
 - 6.3. ניתן להעביר מידע אישי באמצעות חשבונות הענן המיועדים וברישוי משרד החינוך. בעת העברת מידע אישי לסביבת הענן יש לוודא הרשאות גישה רק לבעלי תפקידים רלוונטיים.
7. רק תלמידים ואנשי הצוות החינוכי של המוסד רשאים להשתמש בסביבות הענן. אין לצרף לסביבה גורמים חיצוניים מחוץ לאוכלוסיית החינוך של בית הספר.
8. לתלמידים - שיתוף קבצים ודוא"ל, יתאפשרו לשימוש רק בין המשתמשים הרשומים בסביבה (ולא יהיו פתוחים לציבור).
9. יצירת ממשקים בין סביבות הענן למערכות מידע ואפליקציות חיצוניות יאושרו מראש מול חטיבת הסייבר במשרד החינוך.



הנחיות לשימוש בטוח ביישומי Office 365/G-Workspace

1. הנחיות כלליות:

- 1.1 יש להתחבר לסביבת הענן המשרדית באמצעות ההזדהות האחידה של משרד החינוך בלבד.
- 1.2 **חל איסור מוחלט להשתמש עם חשבון ענן פרטי אישי לצורכי עבודה (לרבות שליחת מיילים מחשבון מייל פרטי כגון Gmail או שמירת מידע משרדי על אפליקציית אחסון פרטית כגון Dropbox).**
- 1.3 יש להימנע משמירת חומרים אישיים במחשבים וסביבת הענן הבית ספרית, המשרד אינו נושא באחריות לחומרים אלו.
- 1.4 אין להשתמש במייל הארגוני כאמצעי לרישום באתרי אינטרנט חיצוניים, כגון בלוגים, רשימות דיוור, אתרי צרכנות וכדומה. לשם כך, יש להשתמש במייל האישי בלבד (כגון: Gmail).
- 1.5 יש להשתמש בסיסמה חזקה (בשירותים שונים - סיסמאות שונות). אין למסור אותה לאף אחד ולא לרשום אותה במקום גלוי.
- 1.6 עדכנו בטלפון הנייד את האפליקציות לגרסה העדכנית ביותר מהחנויות הרשמיות בלבד (Apple Store | Google Play). שיסייעו לכם מפני התקפות זדוניות.

2. שימוש בטוח באפליקציית המייל:

- 2.1 השתמשו בחשבון מייל משרד החינוך (Google/Microsoft) לצרכי עבודה.
- 2.2 הימנעו מפתחת מיילים וקבצים חשודים, ומלחיצה על קישורים חשודים גם אם הם ממקורות מהימנים. לחיצה על קישור עלולה להפעיל או להוריד תוכנה זדונית, לגנוב מידע אישי ולגרום לדלף מידע.
- 2.3 **סימנים לזיהוי מייל חשוד:**
 - 2.3.1 נוסח חובבני של תוכן המייל.
 - 2.3.2 כתובת אתר או אימייל לא רשמיים או עם שגיאות.
 - 2.3.3 בקשה להורדת קבצים או למילוי פרטים אישיים.
 - 2.3.4 הבטחה לפרס או ניסיון פיתוי.
 - 2.3.5 יצירת לחץ ותחושת דחיפות.

3. שימוש בטוח ב-One Drive/Google Drive:

- 3.1 יש לשמור את כל המסמכים והמידע הבית ספרי בתיקייה ממודרת בחשבון הענן הבית ספרי. כוננים אלו מאובטחים ומגובים בשונה מכונני המחשב המקומיים (כגון כונן C או שולחן עבודה) שאינם מגובים.
- 3.2 אין לשתף מידע רגיש הכולל רשומות ופרטים מזוהים עם גורמים שאינם עובדי המשרד או גורמים שאינם מורשים לצפייה במידע.
- 9.1 אין לשתף מסמכים המכילים תוכן רגיש (כגון: ת.ז, שם מלא, כתובת, כתובת מייל, מספר טלפון וכו') באמצעות חשבונות ענן פרטיים (כגון Gmail פרטי) עם גורמים מחוץ למשרד. ככל וקיים צורך להעברת המידע הרגיש למטרות עבודה יש לבצע זאת על ידי שליחת קובץ מוגן בסיסמה באמצעות המייל המשרדי בלבד ויש לשלוח את הסיסמה בערוץ נפרד (שיחה קולית/SMS).
- 3.3 יש לוודא מעת לעת שהרשאות השיתוף, הצפייה וההורדה של מסמכים מעודכנת ותקינה. חשוב לשים לב לדברים הבאים: אפשרות עריכה של מסמך תינתן עפ"י צורך בלבד ויש לבצע בקרת הרשאות מעת לעת למסמכים בדגש על הרשאה בעלי גישה למידע, הרשאת הורדה ועריכה של המסמכים ומתן אפשרות לשיתוף המסמכים עם אחרים.



3.4. היו ערניים לשינויים, במידה והבחנתם בשינוי או בכל דבר המעלה חשד באחד מהקבצים הנמצאים ב-OneDrive/ Google Drive, דווחו בהקדם על כך לרפרנט / ממונה התקשוב במחוז / למפקח.

4. שימוש בטוח ב- Teams/Google Meet/Classroom :

- 4.1. התחברו לפגישה/מערך שיעור מקוון בכל הפלטפורמות באמצעות ההזדהות האחידה של משרד החינוך בלבד.
- 4.2. הפגישה או השיעור ינוהלו על ידי המורה בלבד, השולט בפעולות המשתתפים. השימוש במיקרופון, מצלמה ושיתוף מסך יהיו חסומים למשתתפים כברירת מחדל, עד לאישור המורה.
- 4.3. לפני תחילת פגישה או השיעור יש לוודא כי כלל המשתתפים מזוהים על ידי המורה באמצעות חדר המתנה (Waiting Room) או על ידי אימות בזמן אמת על ידי פתיחת מצלמה.
- 4.4. **ככלל, אין להקליט מפגשים או שיעורים עם תלמידים.** במקרים חריגים בהם נדרשת הקלטה היא תעשה לאחר יידוע המנהל ואישורו על כך בכתב. הקלטה של מפגשים או שיעורים עם תלמידים תישמר בתיקיה ממודרת בסביבת הענן הבית ספרית (כונן דרייב של גוגל או מיקרוסופט בחשבון משרד החינוך).
- 4.5. להנחיות להתנהלות בטוחה בפגישות וידאו ומערכי שיעור מקוונים.

שימוש בטוח בטפסים/סקרים Forms :

1. טפסי/סקרי Forms ישמשו לאיסוף מידע אינפורמטיבי ולרישום, כגון טפסי הרשמה לאירועים, סקרי שירות אנונימיים וכדומה.
2. טפסי/סקרי Forms יהיו מורשים לאסוף מידע אישי כגון שם מלא, טלפון וכתובת דוא"ל לטובת טופס הרשמה בלבד.
3. אין להעלות קבצים לטפסי/סקרי Forms ולא ייאסף מידע מזהה (ת.ז.).
4. בתום איסוף המידע וסיום הצורך בשימוש בנתוני הטופס יש למחוק את המידע שנאסף באמצעותו.

בכל שאלה ניתן לפנות למפקח התקשוב המחוזי או לחטיבת אבטחת מידע וסייבר במשרד החינוך.

במידה ונחשפתם לאירוע אבטחת מידע חשוד או פעילות זדונית יש לדווח על כך באמצעות טופס דיווח על אירוע סייבר (דרך רכז התקשוב | מנהל בית הספר).