



מדריך להורים לחיים ברשת

המנהל הפדגוגי
אגף א' לחינוך יסודי
ירושלים תשע"ג

תוכן עניינים

2.....	הקדמה
3.....	מבוא
5.....	פרטיות - מידע אישי ברשת
10.....	משחקים ברשת
14.....	נשמרים מבריונות מקוונת
18.....	בקרת הורים
25.....	להיות בטוחים עם הטלפון החכם
30.....	שלחתי לך סמס "בוא לאכול"
32.....	איזה תמונה XXX קבלתי בנייד!
34.....	אם את חברה שלי - תגלי לי את הסיסמה שלך
35.....	אינסטגרם, WhatsApp....
36.....	יש דרכים להישמר מקרינה
37.....	לאן ולמי פונים
39.....	מקורות

כתיבה:

הררי לימור- אתיקה ומוגנות ברשת, האגף לחינוך יסודי
אריאלה לונברג- מדריכה ארצית לתקשוב, האגף לחינוך יסודי

קראו והעירו

- מלכה וידיסלבסקי - מפקחת על חטיבות צעירות וממונה על מינהל בית ספרי וסביבות למידה
- המטה הקיברנטי הלאומי

התדריכים הטכנולוגיים נכתבו בעזרת חומרים מבית מייקרוסופט ישראל וחברת גוגל,
בשילוב חומרים שפותחו על ידי רכזי חיים ברשת מהמינהל למדע וטכנולוגיה

הקדמה

המרחב הווירטואלי מזמן הזדמנויות רבות ללמידה ותקשורת למבוגרים ולילדים כאחד, ואולם מרחב זה גם טומן בחובו סיכונים לילדים. הסיכונים העיקריים האורבים לילדים ברשת נובעים מההשפעה שיש לפעילות בלתי מבוקרת ומתמשכת ברשת על התפתחותם הרגשית והחברתית; מפעילות לא אתית ו/או פוגענית שלהם כלפי בני חברת השווים ומפגיעה בהם מצד בני חברת השווים או/ו מצד גורמים אחרים: סוטים ועבריינים והתכנים שהללו מפיצים.

אחד האתגרים בפניהם עומדים מורים והורים כאחד הוא האתגר של יצירת מרחב בטוח ברשת לילדים. כדי ליצור מרחב בטוח ברשת יש צורך בעבודה משולבת של כל הגורמים המעורבים בגידולם ובחינוכם של הילדים: המשפחה, הצוות החינוכי וגורמי חוק.

ממורים והורים נדרש לפתח את היכולת של הילדים להפיק תועלת מרבית מהשימוש באינטרנט ולפעול בו בבטחה ובאופן מוסרי ואתי. בחוברת המובאת בזאת מוצגות הסכנות שישנן ברשת, מוצעות פעולות שהורים יכולים לעשות עם ילדיהם למניעת הסכנות, ובכלל זה פעילויות משחק משותפות ומובאים "טיפים טכנולוגיים".

אנו מקווים שחומרים אלה יסיעו להבטחת גלישה בטוחה לילדיכם

בברכה,

יהודית קדש

מנהלת אגף א' לחינוך יסודי

מבוא

העולם כולו נמצא בקצות אצבעותיהם הקטנטנות... הילדים גדלים לעולם בו הטכנולוגיה היא חלק בלתי נפרד מעולמם. כבר בגיל הרך תינוקות משחקים בטאבלטים ומתבוננים בתמונות ובסרטונים, ואנו עומדים מלאי פליאה כיצד ה -  שלנו מתמצאים בקלות בטכנולוגיה. קצב ההקלדה שלהם כה מהיר שקשה לעקוב אחריו... פעמים רבות אנו מבקשים מילדינו לעזור לנו לעשות משהו במחשב..

זהו עולמם. ומה תפקידנו בעולם זה? האם עלינו להדביק את הפער? ללמוד כל העת ולהתעדכן? לפתוח פייסבוק? לשנות גישה?

הנגישות המתמדת של ילדים צעירים לרשת בעזרת מחשבים, טאבלטים, טלפונים סלולריים, מציפה אותם במידע בכל מקום ובכל זמן. יש להם נגישות למידע שאינו בהכרח מותאם לגילם ונדרשים להפעיל מיומנויות קוגניטיביות של סינון והערכה בגיל צעיר. בנוסף להיחשפות למידע מסוגים שונים, ילדים גם משתפים במידע אישי, בדרך כלל ללא הפעלת שיקול דעת לגבי הדרך בה המידע מוצג, מי נחשף למידע ומה ההשלכות לכך. הם מנהלים תקשורת דיגיטאלית עם מכרים ואחרים.

ילדים מטבעם הם סקרנים וחברותיים. הם לומדים את העולם דרך חקר, גילוי ומשחק, המספק מענה לצרכים רגשיים, חברתיים ואינטלקטואליים בהתאם לשלב ההתפתחותי שבו הם נמצאים¹. בדרך זו הם גם לומדים ומתנסים במרחב הווירטואלי. אך, במרחב הווירטואלי פעמים רבות הילדים גולשים לבד, ללא תיווך של מבוגר. ואולם בשל מאפייני הרשת (זמינות ונגישות המידע מכל מקום; היעדר קשר עין, השטחה חברתית ועוד) ילדים עלולים להיחשף לתכנים לא ראויים ואף לסכנות כגון: תקשורת עם זרים, חשיפת מידע אישי ופרטי, משחקים אלימים, הימורים, פורנוגרפיה, רכישה שלא מדעת, גניבת זהות ופריצה לחשבון משתמש.

הורים שואלים את עצמם: כיצד אנו, המבוגרים, יכולים לתמוך, לעזור, לתווך? ובאילו כלים עלינו לצייד את ילדינו כדי שישמרו על עצמם ועל חבריהם ברשת?

מתוך שיחות עם ילדים, נשמעה פעמים רבות מהם האמירה, כי הם אינם רוצים לספר להורים על מצבים בעייתיים בהם נתקלו ברשת מתוך חשש שההורה "ייקח להם את

■ ¹ הררי, וידיסלבסקי, שמש (2011). [הדרך אל מרחב בטוח](#) – ארבעת המ"מ, אגף לחינוך יסודי

המחשב....", הטכנולוגיה היא אמצעי התקשורת שלהם, הקשר לחברים, לעולם... הם מעדיפים להתמודד לבד עם הבעיות, לא להתייעץ עם הורים ובלבד שלא יהיו מנותקים.

על כן, מתוך הבנת הצורך העז של ילדים בשימוש בטכנולוגיה, על המבוגרים לנקוט בגישה של התערבות מתווכת – תומכת, ולא חוסמת.

מטרת מדריך זה להעמיד לרשות ההורים כלים כדי לחנך את הילדים לגלישה בטוחה ברשת. שימו לב - נושא הגלישה הבטוחה ברשת הוא דינמי מאוד, חלק מהטיפים הטכניים צפויים לאבד רלוונטיות תוך זמן לא רב. לכן מומלץ להורים להתעדכן מדי פעם במנוע חיפוש מידע עדכני בעזרת מילות החיפוש: Parental control, לקרוא מאמרים עדכניים וכן פרסומים רשמיים של הספקיות של מערכות ההפעלה בנושא.

הנחיות יסוד להורים ברשת

 חקרו את המרחב הווירטואלי. אין צורך להיות מקצוענים בו, אבל חשוב להכיר את יתרונותיו וחסרונותיו

 שבו על יד הילדים והתבוננו במה שהם עושים. שאלו אותם לגבי הרגלי הגלישה שלהם, באילו אתרים הם גולשים? עם מי הם מדברים? כיצד הם שומרים על עצמם? הימנעו מטון שיפוטי

 דברו עם הילדים על דרכי ההתמודדות המתאימות כשנתקלים במצבים בעייתיים ועל ההשלכות שלהן

 קבעו יחד כללים לגלישה ברשת והיו עקביים בשמירתם ילדים זקוקים לכללים,

▪ מידע נוסף לכם ההורים ניתן למצוא ב[אתר](#)

פרטיות - מידע אישי ברשת

ברשת האינטרנט פעמים רבות יש מידע אישי רב על אודותינו. את חלקו אנו מוסרים כשאנו מתבקשים לכך (בעת רישום לאתרים ומשחקים) ואת חלקו אנו מכניסים ביוזמתנו. כמו ברשתות חברתיות ובאתרים לשיתוף תמונות, לדוגמה, בהם אנו מעלים תמונות משפחתיות ואישיות, לא תמיד אנו שואלים את עצמנו, מי נחשף למידע זה. על אחת כמה וכמה כשמדובר בילדים. ילדים נוטים בקלות לספק מידע אישי: מספר טלפון, כתובת, תמונה. זאת בכדי להיכנס לאתר מסוים, להשתתף בתחרות או לזכות בפרס מובטח... לעיתים הם אף נותנים לחבריהם את הסיסמה האישית שלהם.

כמו כן מידע אישי רב מאופסן במכשירים טכנולוגיים: מחשב, טאבלט ובטלפון הנייד. מידע זה הוא למעשה תיעוד חיינו האישיים... מעבר לרשימת אנשי הקשר, אנו מאחסנים זיכרונות, תמונות, שיחות, מקומות בהם היינו - ארכיון מדהים של מידע אישי מזהה על אודות המשתמש. מחקר שפורסם על ידי מכון Pew (ספטמבר 2012)², העוסק בשמירה וניהול נתונים האישיים של משתמשים בהתקנים ניידים, מוצא כי קרוב לחמישית מאופן השימוש בטלפון הסלולרי הינו לצרכי גלישה ברשת וניהול מידע אישי. לאור נתון זה גובר הצורך של קובעי מדיניות וכלל הציבור בהעלאת מודעות ומיסוד נהלים ברורים לגבי שמירה על פרטיות וניהול נתונים אישיים.

² http://pewinternet.org/~media/Files/Reports/2012/PIP_MobilePrivacyManagement.pdf

בואו נדבר על זה – מה פרטי ומה ציבורי בחיי הילדים

מה שנתפס כמחייב פרטיות משתנה בהתאם לגיל, מגדר, סביבה, תרבות.

לא תמיד מה שעבורנו המבוגרים הינו מידע פרטי, נתפס ככזה גם עבור הילדים. הם חיים במציאות בה הם נחשפים ברשת לפרסום רב של מידע אישי. הגבולות של הפרטיות מטשטשים. ולכן כשאנו מבקרים את מידת החשיפה של המידע האישי שלהם, אנו עלולים להיתקל בהתנגדות שלהם.

לכן הגישה לנושא חשיפת המידע צריכה להיות מתוך קיום שיח עם הילדים שבו נעשה בירור עמדות שלהם בנושא, העלאת המודעות שלהם לסכנות שבחשיפת מידע מזהה, הבנת ההבדלים בין מרחבי הסביבות השונות והגדרה מחדש של הפרטיות ברשת (כולל אמצעים טכנולוגיים).

איך אני עוזר לילדי להגדיר פרטיות ברשת?

- **הסבירו** לילדיכם ששום דבר שמפורסם באינטרנט אינו נשאר באמת פרטי, אפילו אם הוגדרו הגדרות פרטיות. לכן יש לחשוב היטב לפני שמפרסמים משהו שעלול להזיק להם או להביך אותם.
- **למדו** את ילדיכם לשמור את הפרטים האישיים שלהם באופן פרטי, ועזרו להם להגדיר איזה מידע חשוב להם להשאיר כפרטי כשהם ברשת. מומלץ שילדים לא ישתפו את הכתובת, מספר הטלפון או תאריכי הלידה שלהם.
- **ודאו** שילדים משתמשים בהגדרות הפרטיות ברשתות החברתיות שבהן הם משתתפים. עודדו אותם לחשוב על מערכות היחסים השונות (חברים קרובים, משפחה, מכרים, זרים) ולשנות את הגדרות הפרטיות בהתאם.
- **הזכירו** לילדים להגן על פרטיות חבריהם. העברת שמועה או תיוג וזיהוי מישהו אחר בתמונה, עלולה להשפיע על פרטיותם. אם ילדיכם מתויגים בתמונות של אחרים, הם יכולים להסיר את התיוג, או לבקש לסיר את התמונות.
- **בססו** תנאים בל-יעברו לגבי משלוח רשומות (פוסטים). אין לשלוח בשום אופן ובשום דרך תמונות חושפניות, תמונות של שתיית אלכוהול, סמים או תמונות בעלות הקשרים מיניים.
- **ציינו** שוב ושוב בפני הילדים שהפצת שמועה או דיבור לא נאות על אודות מורה או חבר או כל אדם אחר עלול לרדוף אותם ולהזיק להם במידה שלא תתואר.
- **סייעו** לילדים לחשוב לטווח ארוך על אודות העקבות הדיגיטליים שלהם. מה שנוצר, עשוי לא להיעלם לעולם. אם הם אינם רוצים לראות זאת מחר, עדיף שלא ישלחו את זה היום.

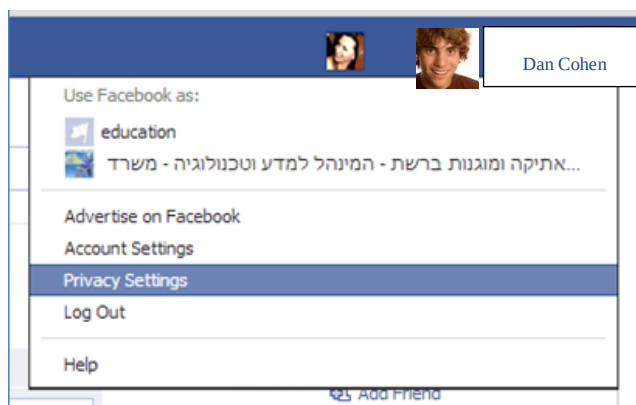
טיפ טכנולוגי !!

איך מגדירים פרטיות ברשת החברתית פייסבוק?

רוב הרשתות החברתיות הציבוריות (ואף אפליקצות כגון אינסטגרם) אינן מאפשרות השתתפות של ילדים מתחת לגיל 13, וזאת, בדרך כלל, נוכח הוראות החקיקה האמריקנית בנושא זה – (COPPA) Children Online Privacy Protection Act אשר אוסרת על אתרי אינטרנט הפונים לקטינים מתחת לגיל 13 לאסוף מידע ללא הסכמה הורית שהתקבלה באופן מהימן.

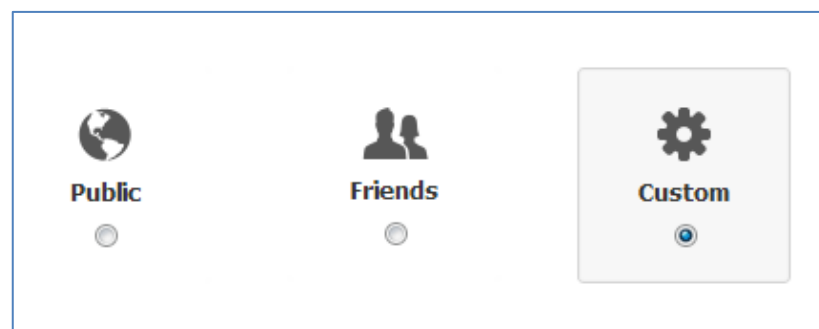
אנו ממליצים לכם ההורים להקפיד על כך ולא לאפשר לילדיכם רישום לאתר מתחת לגיל המצוין בו. הדבר נכון גם לגבי הרשת החברתית פייסבוק. עם זאת, בחרנו להביא בפניכם היבטים טכנולוגיים לשמירה על בטיחות ילדיכם גם ברשתות אלו.

הקליקו על הגדרת הפרטיות (ליד כפתור בית)

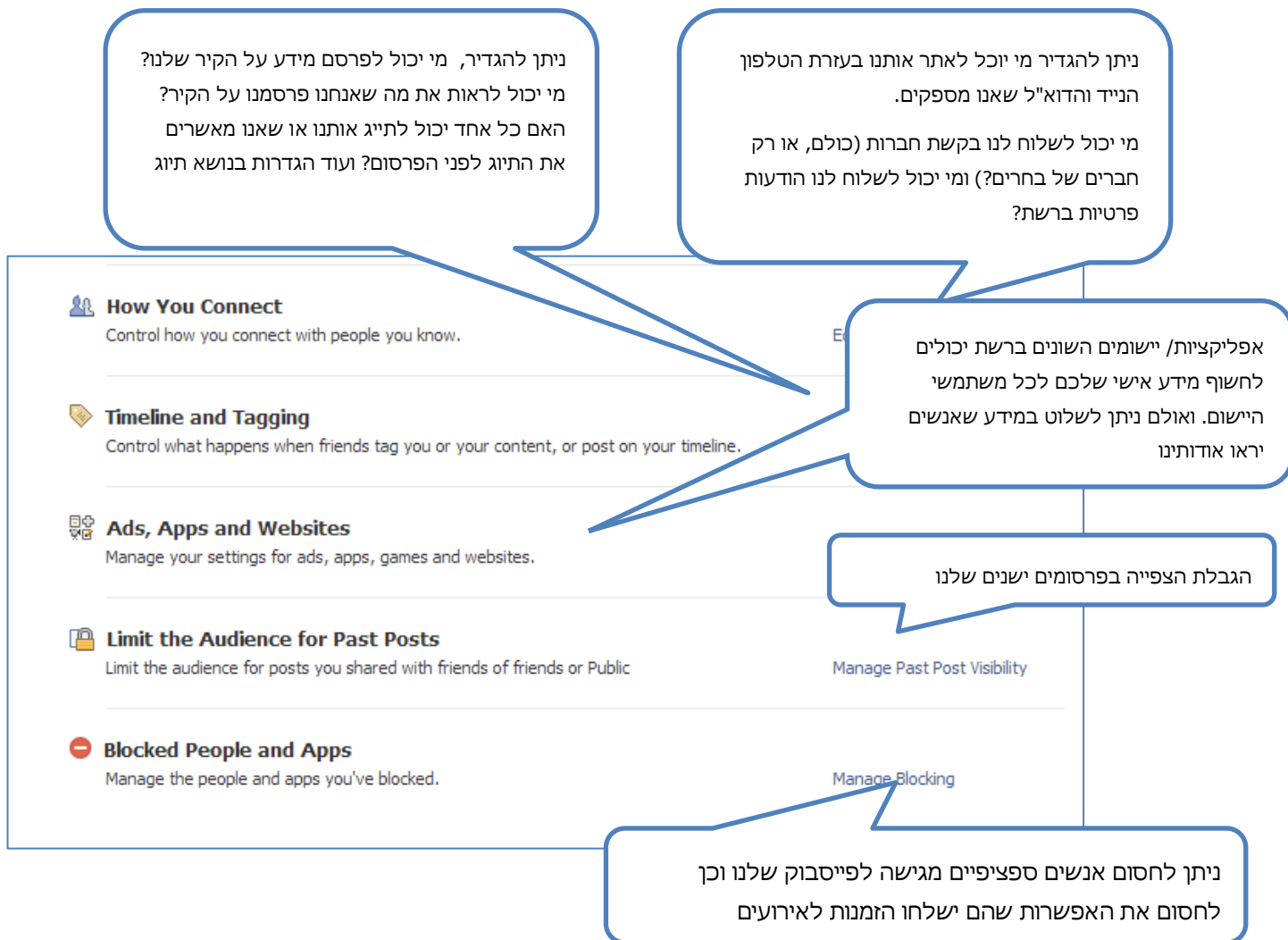


ברירת המחדל של הרשת החברתית הוא: פרסום פומבי "Public"

יש להעביר את הנקודה ימינה ל"מותאם אישית" - Custom (כמו בתמונה מטה) ולהגדיר לגבי כל סוג מידע כיצד הוא יוצג.



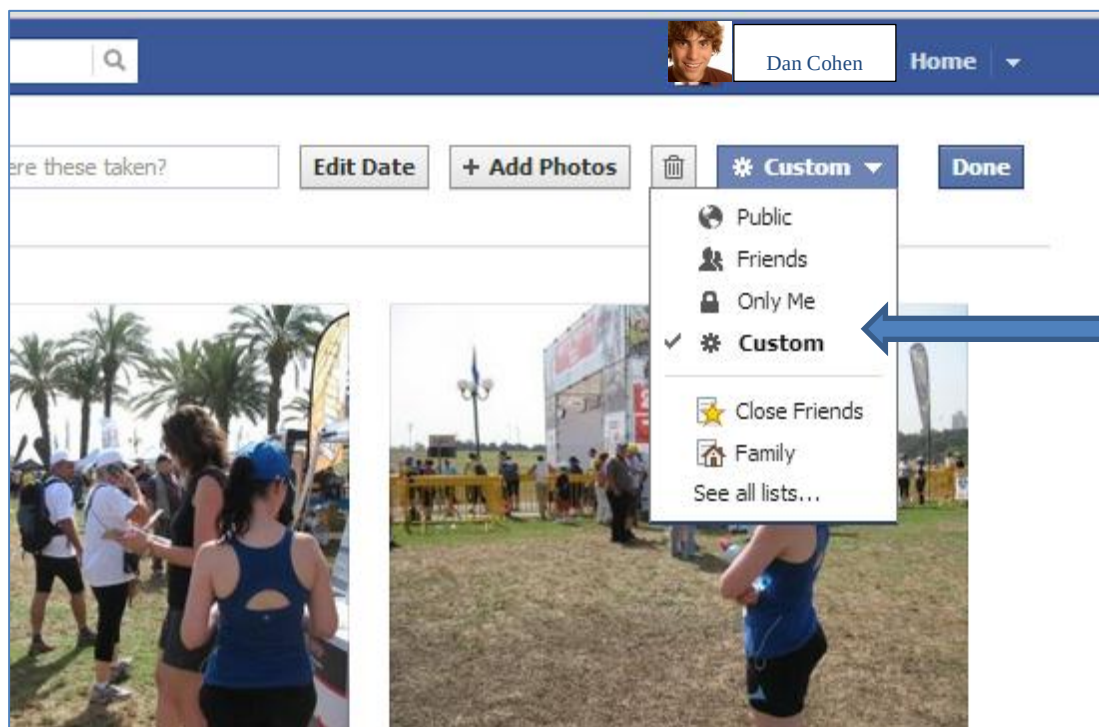
גללו את הדף מטה וראו את האפשרויות השונות לפיהן ניתן להגדיר את פרטיות המידע האישי:



בנוסף להגדרות הנ"ל ניתן למנוע מחברים מסוימים שלנו בפייסבוק או מקבוצות (אותם אנו הגדרנו) מלצפות בתמונה מסוימת שלנו או מאלבום תמונות שהעלינו לרשת.

איך מגדירים מי יראה תמונה/ אלבום תמונות ומי לא?

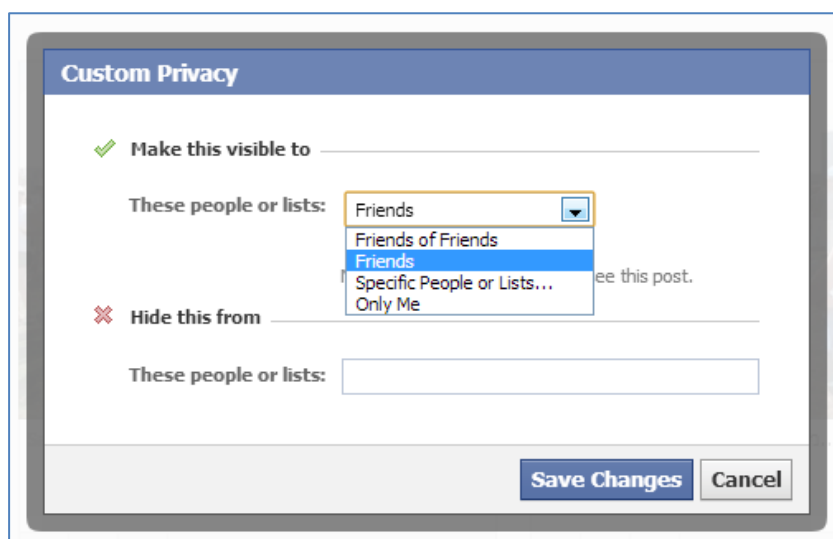
מקליקים על אלבום תמונות. לצד כפתור העריכה הקליקו משולש הבחירה של כפתור התאמה אישית "Custom"



יפתח החלון הבא. ניתן באופן גורף לבחור באחת מהאפשרויות הבאות:

אלבום התמונות יהיה גלוי רק לנו/ לאנשים ספציפיים או קבוצת אנשים (יש להגדירה מראש)/ חברים בלבד/ חברים של חברים.

בנוסף ניתן לבחור באפשרות של הסתרת התמונה או אלבום התמונות מאנשים ספציפיים. ברגע שנרשום את ההתחלה של שמם, המערכת תזהה ותשלים את השם. שימו לב, כבר בשלב יצירת אלבום חדש יש למטה אפשרות לבחור מי יוכל לראות את האלבום



משחקים ברשת

האם ניסיתם להפסיק ילד לשחק או לקרוא לו לפעילות אחרת בדיוק כשהוא עובר שלב במשחק? ... בהחלט לא פשוט...

בשנים האחרונות משחקים דיגיטליים נעשו חלק חשוב ומהותי בחיי הפנאי של ילדים בכל הגילים. ילדים מבלים זמן רב במשחקי מחשב ואינטרנט. למרות ההסכמה שמשחקים יכולים לשמש הן להנאה והן ככלי לימודי בעל עוצמה ללמידה ושיפור כישורי חיים (כגון ניהול זמן, קבלת החלטות, תקשורת בין אישית כמו גם קבלת משוב מידי ושיח עם עמיתים), יש להיות ערניים לסכנות ולחסרונות שעלולים להיות לחלק ממשחקים אלה.

משחקי מחשב או רשת עלולים להכיל מסרים סמויים, תכנים אלימים ושאינם מתאימים לגיל, שימוש בכסף ממשי לשם התקדמות במשחק, והם עלולים להפחית את היכולת לוויסות עצמי ולגרום לאיבוד תחושת הזמן. משחקים חברתיים ברשת יכולים גם לחשוף את השחקנים לאנשים מבוגרים שמחפשים ליצור מגע לא – ראוי עם קטינים כמו קללות ולניבולי פה.

המבחר הרב שקיים במשחקי רשת, מכיל בין השאר סוגת משחק המכונה "משחק רב משתתפים" (Massive Multiplayer Online Role Playing Games). משחקים אלה שמאפשרים למשתתפים בו ליצור זהות רשת בדויה (אווטאר) כשחקנים המשתתפים בהרפתקאות וירטואליות ולעיתים אף משלמים כסף ממשי תמורת ההתקדמות במשחק. חלק מסכנות ההשתתפות במשחקי רשת כוללות סכנות דומות לאלו שכבר הזכרנו והכוללות הפרת הפרטיות ואף פריצה למערכות האבטחה של המחשב או המכשיר הנייד האישי.

רוב המשחקים החברתיים דורשים מן השחקן להיות חלק מקהילה שמשוחחת, מצ'וטטת ושולחת מסרים בזמן המשחק. מטרידנים יכולים להשתמש באינטראקציות הללו כדי לנסות לגלות מידע אישי, גניבת זהות, גניבת אשראי או מגע לא ראוי עם ילדים, תוך שימוש בזהות בדויה³. אך אחת הסכנות ה"שקטות" היא המרצת הנטייה של ילדים לאלימות ולאכזריות. במשחקים כאלה על השחקן לירות, להרוג, להכות ולפגוע באחרים, והוא מתוגמל על פעולות

³ http://www.us-cert.gov/reading_room/gaming.pdf

כאלה. משחקי פעולה רבים מכילים תכנים כאלה המעודדים אלימות ומקמים את הרגישות כלפי האחר. משחקים אחרים מעודדים צרכנות באופן סמוי ואף יכולים להביא להימורים ולהשתתפות בפעילות לא חוקית.

הידעת? לגיימרים שפה משלהם⁴, השפה דינמית ומשתנה – רוצים להכיר במעט...!?

כאשר אומרים....	למה הכוונה?
GG	Good Game משחק טוב נאמר בתום משחק כאות לסיום המשחק והערכה כלפי שאר השחקנים
Noob	כינוי גנאי לשחקנים, מציין שהנך שחקן המשחק גרוע כמו טירון (המונח לקוח מתוך המילה Newbie)
Gamer	שחקן שמשחק הרבה מאוד זמן, נחשב למומחה בתחום
~פעולה~	סימן זה ~ מציין פעולה שהדמות מבצעת- ~יוצאת מהבית וטורקת את הדלת~
"דיבור"	"סימן זה " "מסמן שיחה "זהו, אני לא יכולה יותר, אני הולכת"

מדרג תכני המשחק - כל משחק היוצא לשוק חייב לספק מדרג לפיו הצרכן יחליט אם התוכן ראוי לילדו. זהו סולם לטווח גיל ותוכן. הדירוג במשחק מאשר כי המשחק מתאים לשחקנים מעל גיל מסוים לא על פי רמת הקושי אלא על פי התוכן של המשחק. PEGI (Pan-European Game Information) הינו מודל בו משתמשים בכל רחבי אירופה בהתאם לתמיכה של הנציבות האירופיות בתחום ההגנה על ילדים.

להלן הסימנים המוסכמים על פי מדרג PEGI:

תכני המשחק מתאימים לגילאים האלה ומעלה (המדרג הוא לא על פי רמת הקושי של המשחק אלא על פי תכניו):



⁴מונחים מהשפה בה משתמשים גיימרים:
<http://gamedrone.net/2009/03/11/gamer-lingo-understanding-online-gamers/>

תכני המשחק מכילים תכנים הכוללים:



בנוסף למדרג PEGI קיים מדרג נוסף ושמו: ESRB. מדרג זה הוצא בארצות הברית. לכן משחקים שמיוצרים שם ידורגו על פי מדרג זה. העקרונות של המדרגים זהים, הסימנים נראים קצת שונה.

תוכלו לקרוא על הסימנים המוסכמים שלו באתר: <http://www.esrb.org/index-js.jsp>

על מה עלינו ההורים לשים לב כשהילד משחק במחשב?

- ראו במה הילדים משחקים, שבו לידם ועקבו אחר המשחק עצמו
- לכל משחק יש סימן מוסכם לגבי סוג תוכן המשחק וההתאמה הגילאית שלו. קראו את המדרג ופעלו לפיו
- קבעו יחד עם הילדים את זמני המשחק באופן ברור והקפידו להיות עקביים בכך.
- שוחחו על המשחק עצמו: מה אופיו? אלו תכנים יש במשחק? מדוע הילד אוהב לשחק בו? מה הערך החינוכי שלו?
- שוחחו עם הילד על כללי התנהגות ראויים במשחק ובעיקר בשיח בין השחקים, נמקו ויצרו מסר חינוכי מלמד
- בקשו ממנו להתריע בפניכם על מצבים בהם הוא מזהה שיח לא ראוי

משחקים ולומדים יחד

לפניכם פעילות העוסקת בהעלאת המודעות לחשיבות ניהול הזמן שלנו וההשלכות שיש לגלישה מרובה ברשת על ניהול הזמן. בתום המשחק יש להגיע לסדר יום המוסכם על ההורה והילד.

עזרים

- כרטיסים המייצגים פעילויות שונות שלנו במהלך יממה . כל כרטיס מייצג שעה ביום
- דפי A4 לבנים (משמשים כלוח)
- דבק

כל ילד והורה ידביקו על גבי דף לבן את חלוקת הפעילות לאורך יממה עבור זולתו: ההורה יעשה זאת עבור הילד וההפך. בתום הפעילות, כל אחד יתאר את היממה שלו, ומה הוא למד מזה ויחד יציעו סדר יום המוסכם על הילד וההורה.

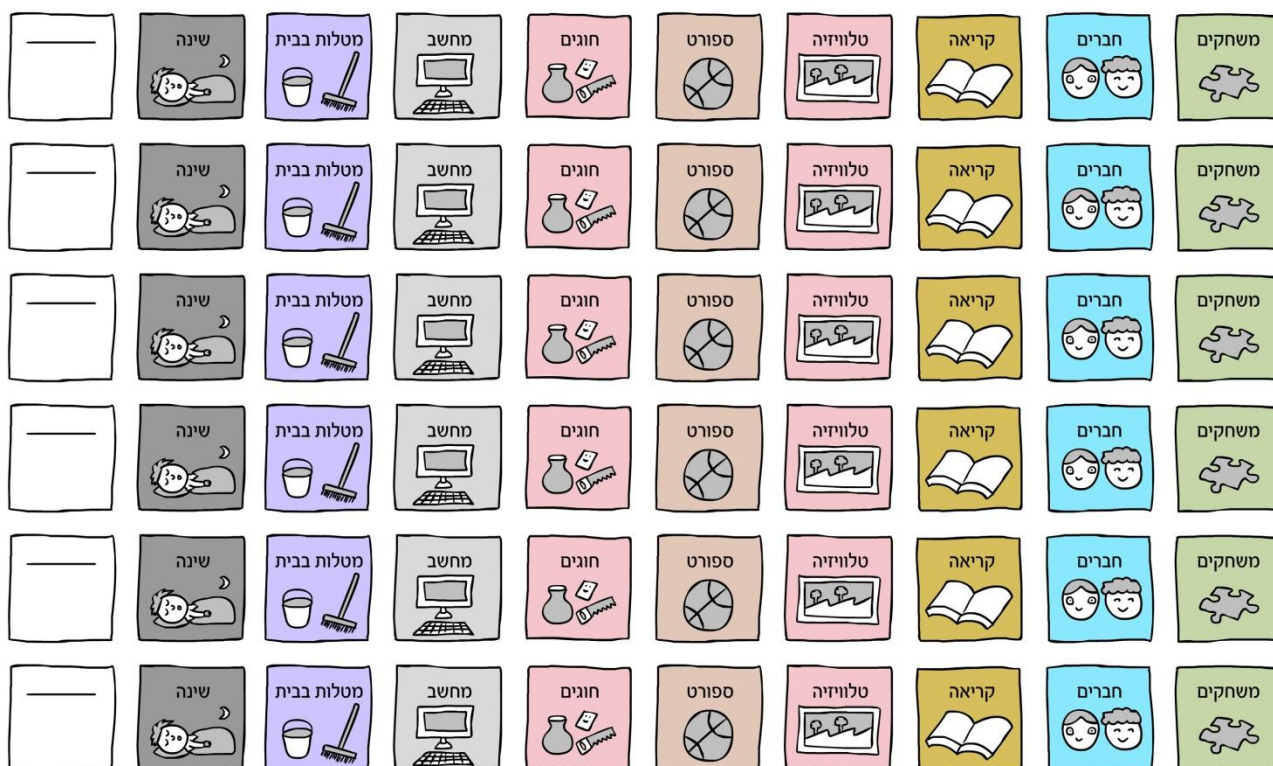
נקודות לשיחה משותפת:

1. כמה זמן אתם מקדישים לשימוש במחשב במהלך היום? מה דעת ההורה והילד על כך?
2. מה ההשלכות של גלישה מרובת שעות לתלמיד על ניהול שעות הפנאי?
3. מה הן הסכנות בגלישה מרובת שעות?

פעילות 3: כרטיסים



לכל זמן ועת לכל חפץ



נשמרים מבריונות מקוונת

בריונות מקוונת היא אלימות לכל דבר, אך כיוון שהיא מתרחשת ברשת, יש לה מאפיינים נוספים. בדרך כלל בריונות חוצה את גבולות מרחב הרשת ופוגעת בילדים גם במרחב הממשי.

בואו נכיר את מאפייני הבריונות המקוונת ונדע כיצד להישמר מפניה:

- **קלות הפגיעה באחר** – מאחורי המסך קל יותר לומר דברים ואף לפגוע בגלל העדר העכבות. בסך הכל כותבים משפט, מקליקים "לייק" או מצטרפים לקבוצה..., כביכול.
- הבריונות המקוונת **נראית לעיני כל** – ברשת "כולם" רואים מה שקרה, לא רק הבריון והנפגע, אלא כל החברים של שני המשתמשים...
- **הפצה רחבה** של המקרה – ניתן להפיץ זאת בקלות כהרף עין ממשתמש אחד למשתמש אחר, בדוא"ל, ברשת החברתית... ניתן להוריד את התמונה הפוגענית ולהפיצה כמו מחלה ויראלית.
- **עוצמת הפגיעה באדם** – כיוון שהחשיפה למקרה רחבה יותר, גם עוצמת הפגיעה הנפשית עמוקה יותר. הדבר חמור עד כדי כך שלעיתים ילדים עוברים מבי"ס לביס אחר, אך גם שם נטפלים אליהם בגלל מה שקרה בביה"ס הקודם...
- **כדור השלג** – מקרה כביכול "פשוט" עלול להיגרר ולהפוך למורכב...
- **אירוע רב משתתפים** – שותפים נוספים מצטרפים באופן טבעי כיוון שכל אחד מגיב, מביע דעה, משמיע הערה, ה... מכאן שמעגל הפגיעה רחב יותר

סיפור שקרה - כדור שלג...

מעשה שהחל במריבה בין שני ילדים וכמעט הפכה לעימות פיסי בין קבוצות: תלמיד בבית הספר רב עם חברו לכיתה. המריבה עברה ממרחב הכיתה אל המרחב הווירטואלי, ושם המריבה עברה לפסים קשים מאוד: נפתחה קבוצה נגד אחד הילדים, נרשמו דברי נאצה, תלמידי הכיתה בחרו במי לתמוך ולא דברו עם הילד האחר. באחד הימים ברשת נקבע מקום מפגש לעימות פיזי. הדבר הובא לידיעת המחנכת, התערבות נכונה שלה יחד עם צוות "חיים ברשת" מנעה הסלמה של המצב. שיח גלוי על הדברים ועצירת הדברים מהמשך אלימות נוספת.

בואו נדבר על זה – הנחו את ילדיכם

- לא להגיב לבריונות ברשת
- לצלם את המסך כהוכחה לבריונות שארעה
- לידע מיד במה שקרה חבר או אדם מבוגר עליהם הם סומכים. ראו [למי ניתן לפנות](#)
- דווחו גם באמצעים טכנולוגיים על כל מקרה של פגיעה במישהו



על מה עלינו כהורים לשים לב?

אם הילדים ממזערים את המסך במהירות כשנכנסתם לחדר, ייתכן שהם רוצים לשמור על פרטיותם, או שהם חוששים מתגובתכם. נצלו את ההזדמנות כדי לשוחח עימם על הנושא.

שימו לב כמה זמן הילד גולש במחשב – חשוב כי לא יהפוך את הפעילות במחשב למרכיב הבלעדי בחייו. אם לדעתכם ילדיכם מבלה זמן רב מדי על המחשב, עזרו לו למצוא עיסוקים אחרים: פעילות גופנית, אמנויות, התנדבות ועוד.

שימו לב לשינוי במצב הרוח של ילדיכם - שינוי קיצוני עשוי להעיד על מצוקה. שוחחו ובררו מה קורה.

משחקים ולומדים יחד

לפניכם פעילות שמטרתה לעודד את הילדים לפנות אליכם ההורים ולהתייעץ בנושאים הקשורים לגלישה ברשת

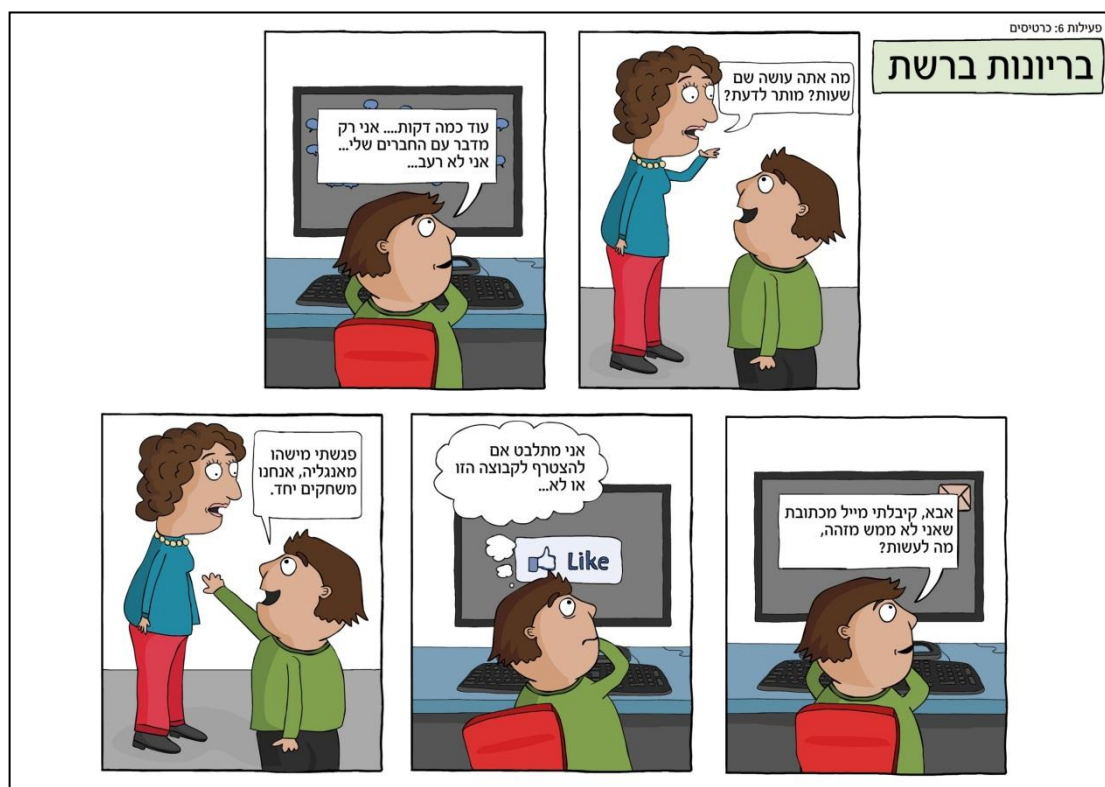
עזרים:

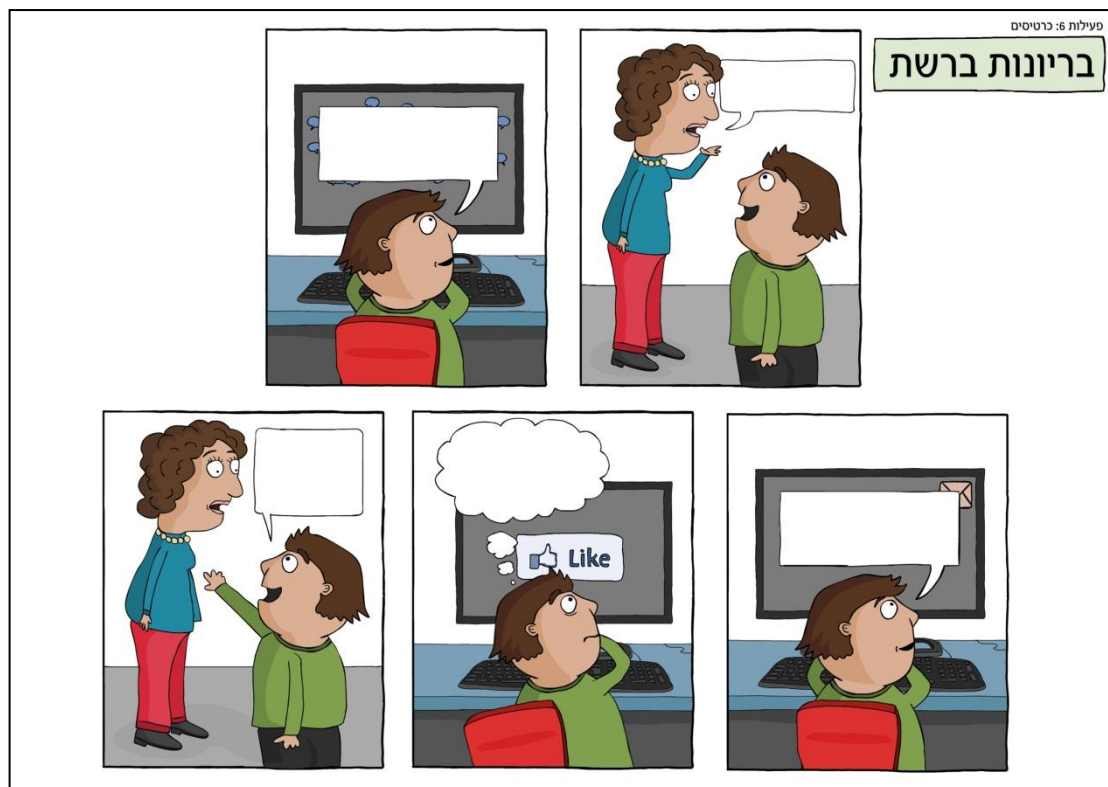
- כרטיסים בהם אמירות של הורים
- כרטיסים ריקים להשלמה

על הילדים למלא את הכרטיסים הריקים ולכתוב בהם משפטים אותם הם אומרים להוריהם בהקשר למחשב. הילדים יניחו את הכרטיסים במרכז, כל אחד בתורו ירים את הכרטיס, יתאר מה הוא רואה. ההורים ישוחחו עם הילדים על מה שהם מציפים

נקודות לשיחה:

- איך אתם מרגישים כשזה נאמר על ידינו (ההורים)?
- מדוע לדעתכם הדברים הללו נאמרים?
- כיצד אתם פועלים?





בקרת הורים

רשת האינטרנט היא מקור הנאה גדולה לילדים. ישנם ברשת מספר עצום של אתרים איכותיים ומעניינים, מאמרים, תמונות, משחקים ועוד פעילויות רבות ומהנות. הבעיה בפעילות באינטרנט, כמו בהרבה תחומים אחרים, היא שלא תמיד ניתן לדעת מתי עוברים הילדים לפעילות שעלולה לגרום להם נזק.

כמו כן פיקוח על ילדים באינטרנט עלול להיתפס כחדירה לפרטיות הילדים. יש דעות רבות בעד ונגד בנושא זה. בכל אופן, מומחי אינטרנט, המודעים לסכנות בתחום, ממליצים לפקח על פעילות הילדים, במיוחד לאור העובדה שאם הילדים מסתבכים, האחריות כמובן נופלת על ההורים.

פיקוח על זמני השימוש במחשב

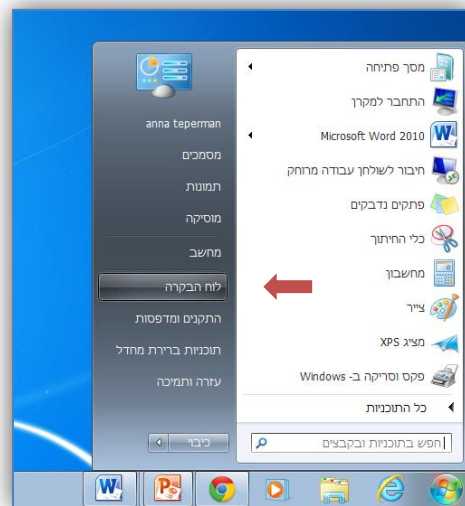
מומלץ לפקח על שעות השימוש של הילדים במחשב.

ניתן להגדיר מגבלות זמן כדי לקבוע את השעות שבהן מותר לילדים להיכנס למחשב. מגבלות זמן מונעות מילדים להיכנס למחשב בשעות שהוגדרו. באפשרותכם להגדיר שעות כניסה שונות עבור כל יום בשבוע. אם הם מחוברים כשהזמן שהוקצב להם מסתיים, המערכת תוציא אותם באופן אוטומטי.

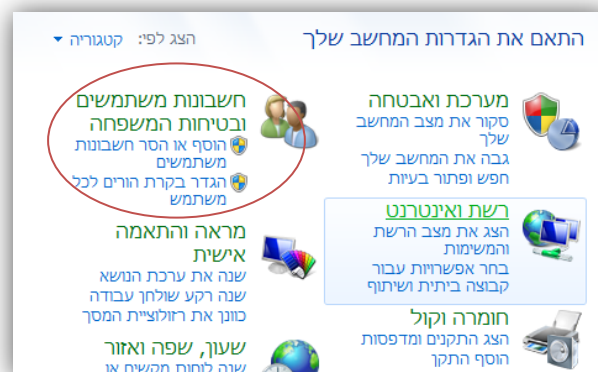
טיפ טכנולוגי !!

הגדרות אבטחה - ההנחיות הטכניות הללו הן עבור ווינדוס בגרסה 7

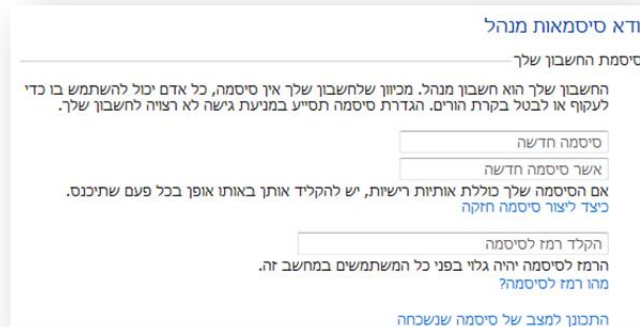
1. הגדר מגבלות זמן ספציפיות לשימוש של ילדיך במחשב. פתחו את 'בקרת הורים' על-ידי לחיצה על לחצן התחל, לחיצה על **לוח הבקרה** ולאחר מכן, תחת **חשבונות משתמשים ובטיחות המשפחה**



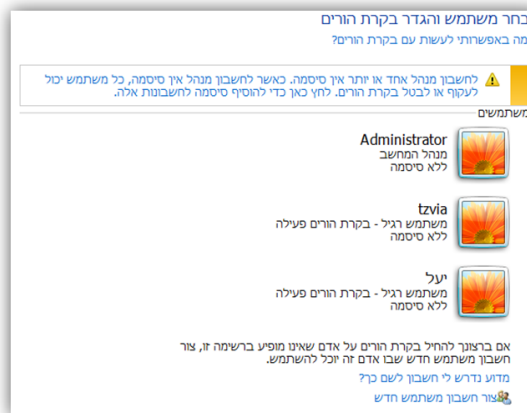
2. לחיצה על הגדר בקרת הורים לכל משתמש .



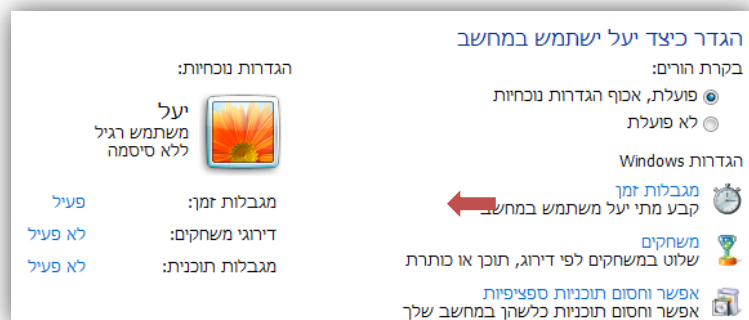
3. אם אתם מתבקשים לספק סיסמה או אישור של מנהל מערכת, הקלידו את הסיסמה או ספקו אישור.



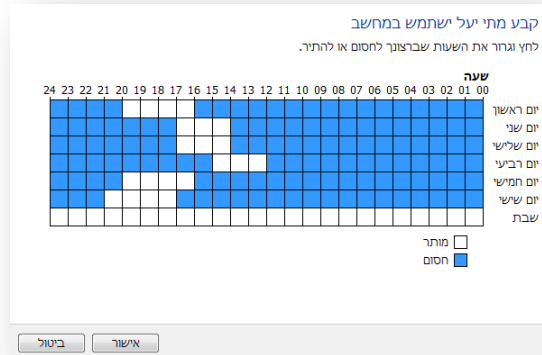
4. לחצו על החשבון שעבורו ברצונכם להגדיר מגבלות זמן.



5. תחת בקרת הורים, לחצו על פועלת, אכופ הגדרות נוכחיות.



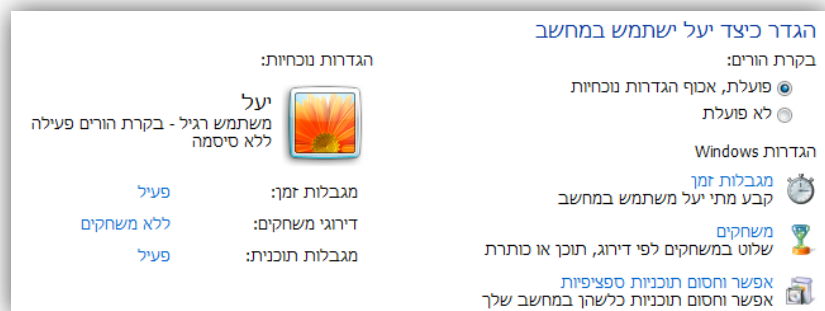
6. לחצו על מגבלות זמן. ברשת, לחצו וגררו את השעות שברצונכם לחסום או להתיר ובסוף לחצו על אישור.



ניתן להדפיס את מערכת שעות במחשב על מנת לעדכון הילדים הלוח הזמנים.

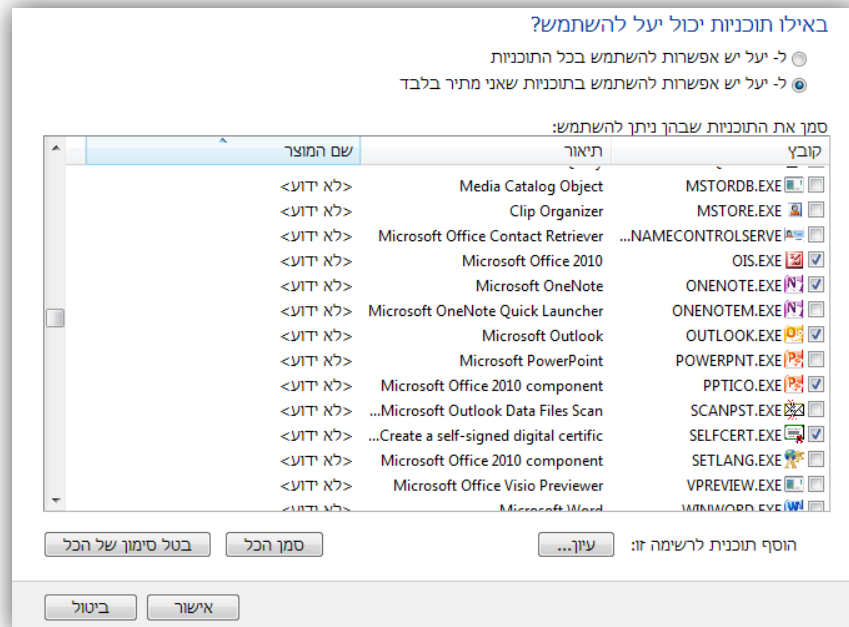
מניעה מילדים להשתמש בתוכניות מסוימות

באפשרותכם להשתמש ב'בקרת הורים' כדי לקבוע באילו תוכניות ספציפיות יוכלו ילדיכם להשתמש. לדוגמה, אם אתם משתמשים בתוכנית כדי לעקוב אחר ענייני הכספים שלכם, באפשרותכם למנוע מילדכם לפתוח אותה ולהציג את המידע הפיננסי.



1. באותו חלון של הגדרות זמן ניתן לקבוע באילו תוכניות ספציפיות יוכלו ילדיכם להשתמש. תחת **בקרת הורים**, לחצו על **פועלת, אכופ הגדרות נוכחיות**.

2. לחצו על **חסום תוכניות ספציפיות**.



3. לחצו על 'לשם האדם יש אפשרות להשתמש בתוכניות שאני מתיר בלבד'.

4. בחרו את התוכניות שברצונכם לאפשר. אם התוכנית הרצויה אינה מופיעה ברשימה, לחצו על **עיון** כדי לאתר את התוכנית

באפשרותכם להשתמש ב'בקרת הורים' כדי לקבוע באילו משחקים מותר לילדיכם לשחק במחשב. באפשרותכם לחסום את:

- כל המשחקים.
 - משחקים ספציפיים לפי בחירתך.
 - משחקים ספציפיים בהתבסס על דירוגי גיל.
 - משחקים ספציפיים בהתבסס על דירוגי תוכן.
- ניתן להשתמש גם בשילוב של ארבע שיטות אלה.

שלוט בסוגי המשחקים שבהם ל- יעל יש אפשרות לשחק

אם למשחק אין דירוג, האם יעל יוכל לשחק בו?

☒ הטר משחקים ללא דירוג
☐ חסום משחקים ללא דירוג

באילו דירוגים מותר ל- יעל לשחק?
 ה- Entertainment Software Rating Board מגדיר דירוגים אלה.



EARLY CHILDHOOD	EVERYONE	EVERYONE 10+	TEEN	MATURE	ADULTS ONLY
C כותרים בדירוג EC - Early Childhood כותרים בקטגוריה זו אינם מכילים תוכן שעשוי להחשב לבלתי הולם בעיני הורים.	E כותרים בדירוג E - Everyone כותרים בקטגוריה זו עשויים להכיל אלימות מינימלית, מעשי קונדס קומיים ו/או שפה מתונה.	E10+ כותרים בדירוג E10+ - Everyone 10 and older כותרים בקטגוריה זו עשויים להכיל יותר אלימות מתונה, אלימות בסרטים מצוירים או אלימות פנטזיה, שפה מתונה ו/או רמיזות מיניות מינימליות.	T כותרים בדירוג T - Teen כותרים בקטגוריה זו עשויים להכיל תוכן אלים ו/או שפה מתונה או בוטה.	M כותרים בדירוג M - Mature כותרים בקטגוריה זו עשויים להכיל נושאים מיניים למבוגרים, אלימות מוגברת ו/או שפה בוטה.	AO כותרים בדירוג AO - Adults Only כותרים בקטגוריה זו עשויים להכיל תוכן שמתאים למבוגרים בלבד.

←

5. לאחר בחירת המשחקים יש ללחוץ על אישור.

כדאי לצפות בסרטון וידאו, ראה  **וידאו: שימוש בבקרת הורים.**

טיפ טכנולוגי !!

אבטחת מידע בעזרת דפדפנים

דפדפן (Browser) הוא סוג של תוכנה המציגה דפי אינטרנט ומאפשרת לעבור בין דפים שונים (פעולת הדפדוף מכונה גלישה) ולעתים אף לתקשר עם תוכן הדפים. דפדפנים נפוצים: Explorer, Chrome, Safari, FireFox ועוד

לכל דפדפן אפשרויות שונות של הגדרות אבטחה כך שנוכל להגדיר או למנוע גישה לתוכן מסוים עבור ילדינו.

לדוגמא בדפדפן אקספלורר עליכם לגשת לכלים – אפשרויות אינטרנט – תוכן – מסננים – אתרים מאושרים ושם להגדיר אתרים רצויים ואסורים.

בכל דפדפן מיקום ההגדרות מעט שונה, חפשו זאת בסרגל הדפדפן או ב'עזרה'.

שימו לב – בנוסף לשינוי בהגדרות הדפדפן, חשוב להגביל את השימוש של הילד רק לדפדפן בו הגדרתם את [הגדרות האבטחה](#).

להיות בטוחים עם הטלפון החכם

הטלפון הנייד הפך להיות חלק בלתי נפרד מחיי היום-יום. הלשכה המרכזית לסטטיסטיקה פרסמה בפברואר 2012 כי במדינת ישראל ל- 97.5% משקי בית עם ילדים יש טלפון נייד אחד לפחות ול-86.9% יש שני טלפונים ניידים ויותר, ואילו במשקי בית ללא ילדים ל-87.7% יש טלפון נייד אחד לפחות ול-54.7% יש שני טלפונים ניידים ויותר⁵.

ההתקדמות הטכנולוגית תרמה לשינוי ייעודו של מכשיר הטלפון הנייד ממכשיר לתקשורת בלבד בו משוחחים ושולחים הודעות טקסט, למכשיר אינטראקטיבי בו מאזינים למוסיקה, משחקים, משתפים תמונות ווידאו וגם מאחזרים מידע רלוונטי. רשת האינטרנט, הזמינה בכל זמן ובכל מקום מאפשרת למשתמשים להיות מחוברים באופן תמידי לרשתות חברתיות לעדכן בזמן חי כל אשר עולה על רוחם, דבר המהווה כלי טכנולוגי בעל חשיבות עצומה עבור אנשים צעירים ובכלל.

עבור ילדים ואנשים צעירים בפרט הטלפון הנייד הוא פריט חיוני אותו הם נושאים בכל עת ולכל מקום. מכשיר זה הינו לעיתים מכשיר המדיה הפרטי הראשון עבור צעירים שמשמש רק אותם ומכיל את המידע הפרטי שלהם, את עולמות העניין שלהם ואת הקשר הנחוץ להם עם קבוצת השווים (חברים). ואילו עבור ההורים טלפון נייד הוא אמצעי לתקשורת עם הילדים בכל זמן ומכל מקום שבו הם נמצאים. לילדים הוא מספק מענה לצורך לשמור על קשר עם אחרים ולהיות מעודכנים תמידית.

שימוש מושכל בטלפון הנייד כולל שמירה על פרטיות המידע האישי ומודעות לעקבות דיגיטליים, שימוש מושכל בשירותים מבוססי מיקום, פרסום והפצת מידע, מיסרור ובריונות, קרינה ושמירה על בריאות המשתמש.

לדאבוננו, הדרך הפשוטה ביותר לחדור לפרטיות ולמצוא פירטי מידע היא לקחת את הטלפון של מישהו כשהוא לא שם לב... אנו עדים לתופעה של ריבוי גניבות של טלפונים סלולאריים כדי למזער נזקים כדאי לעודד את הילדים לקבוע סיסמא לטלפון (אותו המשתמש יתבקש להכניס בכל פעם שהטלפון חוזר ממצב "רדום") כדאי שההורים יהיו שותפים לסיסמה. יש מספר אפליקציות המאפשרות למחוק את הנתונים בטלפון לאחר שהטלפון נגנב, דוגמת: [Find my iPhone](#) או [Where's My Droid](#).

⁵ http://www.cbs.gov.il/reader/newhodaot/hodaa_template.html?hodaa=201211045

ניתן להגיע בקלות בטלפון נייד (כמו במחשב) לתוכן פוגעני, פורנו ותוכנות זדוניות. יש אפליקציות בהם ניתן להתקין בקרת הורים כדי למנוע מלהגיע לקישור הלא נכון...בנוסף, יישומי ניטור הורים מאפשרים להורה לראות את היסטוריית הגלישה של הילדים מפורטל אינטרנט מרוחק.

דוגמאות לאפליקציות ניטור ובקרה (חלקן חנימיות וחלקן כרוך בעלות): McAfee Family Protection, AVG, Net Nanny, K9 Web Protection Browser

בטלפון הנייד קיימים [שירותים מבוססי מיקום](#). אלו מאפשרים לחברות הסלולר לזהות את מיקום הנייד ולספק מידע למשתמש על אודות מיקום המכשיר בהתאם לצורך של המשתמש: נווטן (GPS) דיווחי תנועה (Waze), אירועים בסביבה, סרטים, מסעדות באזור, חברים בקרבת מקום ועוד. אפשרויות אלו מספקות למשתמש מידע עדכני בהתאם למיקומו הגיאוגרפי. אולם, שירותים אלו גם עלולים לספק מידע לאחרים גם שאיננו מעונינים בכך. בנוסף, שירותי המיקום מאפשרים לתייג את המקום בו נמצא המשתמש על ידי העלאת תמונה או סטטוס שפורסמו באמצעות הסמארטפון. כלומר: ניתן לראות את המיקום המדויק של המשתמש ואף לעקוב אחריו. באמצעות תוכנות המשתמשות בשירותי המיקום, ניתן לצפות במסלול בו הולך המשתמש ולהעביר את המידע לאחרים.

בשנים האחרונות יש הצפה של טכנולוגיות המאפשרות לתקשר באמצעות מכשירים ניידים בדרכים שונות (WiFi, GSM, GPS...). הטכנולוגיות הללו מאפשרות למשתמש לחקור את סביבתו, לאתר אובייקטים (משטרה, תחנת דלק, סופרמרקט מסעדה) לפי צרכיו, לבדוק באיזה מסלול עדיף לו לנסוע, להשוות מחירים בחנויות קרובות, לקבל דיווח על מדדי זיהום אוויר או לדעת מתי יגיע האוטובוס הבא והיכן הוא נמצא. לכל אותם יישומים משתמשים במרכיב מרחבי של איכון המיקום שבו נמצא המשתמש (Schiller and Voisard 2004).

צפייה בפרטי תמונה שצולמה באמצעות הסמארטפון והועלתה לרשת, מאפשרת לדעת היכן התמונה צולמה (מיקום מדויק). כך ניתן לאסוף נתונים על המשתמש, ניתן לדעת היכן הוא גר, היכן עובד ומהו מסלולו היומיומי.

אחד מהיתרונות הגדולים של שירותים אלה לגבי הורים, הוא היכולת לאתר או לשמור על "קשר עין" עם ילדים (ניתן לקבל הודעה כאשר ילד עוזב או מגיע למקום כלשהו כמו לביה"ס או הביתה).

ואולם עולות שאלות נוספות לגבי פרטיות המידע. חברות מסחריות המציעות שירות מבוסס מיקום מאחסנות לעיתים קרובות מידע שעלול להיות רגיש, פרטי ואישי. כך דווח במחקר

שנערך מטעם רשת התקשורת האמריקאית AT&T כי מידע מסוים על אודות מיקום משתמשים דלף לגופים מצד שלישי בכל הרשתות החברתיות שנחקרו, כגון, Facebook, Flickr, Twitter, MySpace. זאת על אף נהלי הפרטיות שנהוגים ברשתות אלו.⁶

לצורך מענה על השאלות הנוגעות לפרטיות וכדי להתגבר על הסיכונים הכרוכים בדיווח על אודות מיקומם של המשתמשים, מבקשים רוב השירותים את אישורו של המשתמש לצורך רישום, תיעוד, שימוש או אזכור מיקומו. מנגנון זה בעייתי בפני עצמו משום שעצם התיעוד יוצר רישום עבור המיקום. בנוסף, עבירות רכוש שנעשו במקרים של שיתוף מיקום על ידי המשתמש (פריצה לבתים של אנשים שכתבו חוויות ממקומות שונים בעולם באופן פומבי) הובילו גם חלק מחברות הביטוח לשלול זכאות לפיצוי לאלו ששיתפו מידע זה.⁷

אנשים מבוגרים בכלל וילדים בפרט מדווחים באופן תדיר על אודות מיקומם, אך שוכחים כמה מידע אישי מפורסם בזאת ועד כמה עשוי הדבר להוות בעיה אפילו בשירותים מאובטחים יותר. המשתמש (בוגר או ילד) חושב לתומו כי הוא רק מיידע את חבריו היכן הוא נמצא, אך אם המידע הזה יכול להיות נגיש לאנשים זרים, אין לדעת מה הסיכון הכרוך בזאת.⁸

אחד הפתרונות המוצעים הוא הרחבת שליטתו של המשתמש בנתונים העלולים לאכן את מיקומו ללא הסכמתו. לרוב השירותים מבוססי המיקום יש הגדרות פרטיות רחבות יחסית (עם אפשרויות שונות) כך שהמשתמש יכול להבטיח כי רק אותם אנשים שהוא חפץ שיראו את מיקומו, אכן יראו זאת. לשירותים אחרים יש הגדרות ספציפיות יותר (לאפשר לך להגדיר את מקום הימצאותך כך שאתה מאוכן במקום אחר ממה שאתה נמצא באמת...) או להגדיר שאנשים מסוימים יראו שאתה נמצא במקום מסוים ואנשים אחרים יראו שאתה במקום אחר...

איך מופעלים שירותי המיקום?

שבב של GPS נמצא בכל מכשיר של טלפון חכם הוא מסמן את המכשיר ומאפשר מעקב אחריו. בהרבה מאוד אפליקציות המשתמש מתבקש להפעיל את שירותי המיקום בעת השימוש באפליקציה.

⁶ ראו ערך "שירות מבוסס מיקום" בוויקיפדיה
http://he.wikipedia.org/wiki/%D7%A9%D7%99%D7%A8%D7%95%D7%AA_%D7%9E%D7%91%D7%95%D7%A1%D7%A1_%D7%9E%D7%99%D7%A7%D7%95%D7%9D

⁷ <http://net.nana10.co.il/Article/?ArticleID=733675>

⁸ <http://www.bbc.co.uk/webwise/guides/parents-location>

טיפ טכנולוגי !!

מה לעשות?

כאשר מפעילים בפעם הראשונה את הטלפון החכם (סמארטפון) מתקבלת הודעה לפיה יש לאשר את השיתוף בשירותי המיקום. המשתמש נשאל אילו מהאפליקציות שברשותו ישתתפו בשירותי המיקום.

בנוסף, כל אפליקציה חדשה המשתמשת בשירותי מיקום מחויבת לבקש אישור להשתמש בשירותי המיקום בכל פעם שמפעילים את האפליקציה.

למשל: הנה תמונה מתוך אפליקציית "עכבר העיר" לפיה המשתמש מתבקש לסמן אם הוא מעוניין להשתמש בשירותי המיקום או לא:

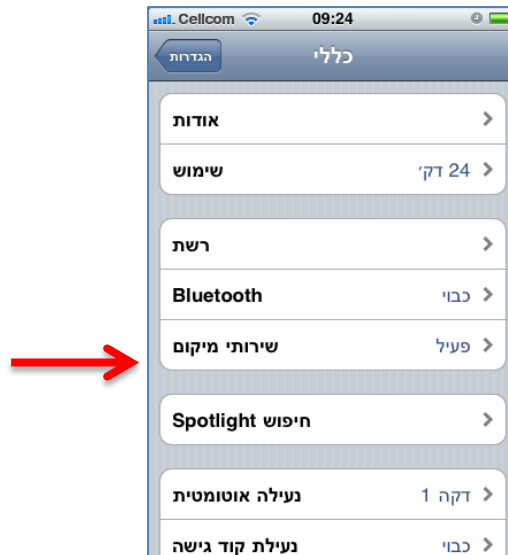


חשוב לשים לב להודעות אלו ולא להקליק באופן אוטומטי על אישור – עלינו להחליט מתי אנו משתמשים בשירותי מיקום ומתי לא.

אם אישרנו את השימוש בשירותי מיקום ואנו רוצים לבטלם, ניתן לבטל זאת על ידי הקלקה על:

הגדרות = > כללי = > שירותי מיקום = > כיבוי

(ניתן לעשות זאת בכל מכשיר, צילומי המסך הללו לקוחים מתוך מכשירי האיפון)



שימו לב - ברירת המחדל של כל מכשיר נייד היא כי השימוש במצלמה מוגדר כפועל על שירותי מיקום. כדי לנטרל זאת יש להקליק על:

הגדרות = < כללי = < שירותי מיקום = < מצלמה = < כיבוי



שימו לב, אם מעלים לרשת תמונה שצולמה על בסיס שירותי מיקום, ניתן לדעת היכן התמונה צולמה. אפשרות עוקפת לנטרל זאת (אם לא כיבינו את ההגדרה של שירותי מיקום) היא לאחר צילום התמונה, לצלם את התמונה שוב במכשיר עצמו ולהעלותה לרשת.

שלחתי לך סמס "בוא לאכול"...

מסרונים (Short Message Service, SMS) הינם דרך מהירה ופשוטה לתקשורת טקסטואלית. הודעות טקסט מהוות מרכיב במערכות התקשורת בטלפון הנייד ובאינטרנט.

אחד המאפיינים של תקשורת בעזרת מסרונים הינו העברת מסרים מהירה. הדבר יוצר שינוי בשפה,⁹ עד כי יש המחשיבים את שפת המסרונים כשפה נוספת המשתמשת ב- 160 התווים הקיימים במקלדת כדי ליצור קיצורים וסימנים חדשים שמגבירים את משמעות התוכן וחוסכים זמן.

הידעת? - אחד מתוך שלושה ילדים (עד גיל 16) שולח יותר מ-100 מסרונים ביום, 3000 מסרונים בחודש (Pew, 2010).

צעירים משתמשים בתצורות המקוצרות הללו לעיתים קרובות בכדי להעביר מסר ארוך במעט הקלקות וכן בכדי לבודל את עצמם מעולם המבוגרים וליצור שפה משל עצמם.

השפה לקוחה פעמים רבות מראשי תיבות - אותיות הלקוחות מתוך המילים במשפט, לעיתים בערוב של מילים ומספרים או סימנים מחוברים יחד שמזכירים מחווה או רגש על ידי הפיכת הסימן על צדו.

דוגמאות פופולריות:

קיצור אותיות	פירוש
LOL	Laughing out loud "הצחקת אותי"
bbb	Bye bye baby "להתראות"
CU	See you "להתראות"
BFF	Best friends for ever "חברות טובות לנצח"
:)	סמיילי – חייכן
(;	קריצה
9-;	טעים
*-;	נשיקה

לעיתים, מסרונים שיש בהם אמוטיקונים הם סוג של קוד המבטא השתייכות לקבוצה מסוימת של חברים או תת-תרבות, דבר היכול להיראות מוזר ובלתי קריא לחלוטין עבור כאלה שאינם

⁹הררי, ל. (2010). [\(פנות חד! את במדיה הדיגיטאלית ומקומן בתכניות הכשרת המורים](#). מכון מופת, ביטאון 44 עמ' 43-46

משתייכים לקבוצה. יש הטוענים כי צורת ביטוי זו היא השטחת השפה העברית. יש הרואים בקיצור השפה הפחתה של מילים ואף חוסר כבוד כלפי נורמות כתיבה מקובלות והשפעה רעה על היכולת הלשונית. לעומת זאת, יש מחקרים המראים ששימוש תכוף בתצורות הללו דווקא יכול להיות קשור לרמה גבוהה של קריאה וכתיבה. יש הטוענים שההתעסקות עם השפה הכתובה בכל דרך שהיא עוזרת לפתח מיומנויות אלה¹⁰.

יודעים מה כתוב כאן?

כל הק!9*ם !ה!ק!9ת9נ ג*Wם ה!*ם 2גן ל T*ה3yNה.

תביאו משו :-9

LOL bbb

¹⁰<http://pwptechnology.pbworks.com/f/Writing,+Technology+and+Teens+-+Pew+Research+Center.pdf>

איזה תמונה XXX קבלתי בנייד !

מסרור מיני (Sexting) - הינו שליחת הודעות בעלות אופי מיני באמצעים דיגיטליים: טלפון סלולרי או אמצעי טכנולוגי אחר. מסרים מידיים. נוהג של שליחת תמונות ורמיזות מפורשות גדל, במיוחד בקרב בני נוער. מה אם כן הבעיה?

הקלות שבה אותם מסרים יכולים להיות מופצים מהווה מקור לדאגה. תמונה המשותפת לשני אנשים, יכולה להיות מופצת באופן ויראלי ברשת. אלו משאירות טביעת רגל דיגיטלית ועלולים להוות מקור פגיעה באחר

תדירות תופעת המסרור המיני תלויה בגיל, בתרבות ובסוג המדיה (מסרונים בטלפון נייד, דואר אלקטרוני, רשתות חברתיות). ככלל נמצא כי ככל שגיל הילדים עולה, כך עולה הסיכון למעורבות במסרור מיני (Kowalski, Limber & Agatston, 2008). במחקר שנערך בארה"ב בשנת 2009 נמצא כי 4% מבני הנוער בגילאי 12-17 שלחו תמונות מרמזות מינית או תמונות עירום של עצמם למישהו דרך מיסרון. 15% מבני הנוער בגילאים הללו קיבלו תמונות מרמזות מינית או תמונות עירום של עצמם למישהו דרך מסרון בטלפון הנייד. בני נוער שמשלמים בעצמם את חשבון הטלפון עשויים יותר לשלוח הודעות מיניות (17% מאלה שמשלמים בעצמם את החשבון, 3% מאלה שאינם משלמים בעצמם או רק חלק מהחשבון).

יש שלושה תסריטים עיקריים המהווים רקע לשליחת מסרונים מיניים: 1. מיסרור בעל אופי מיני בין בני זוג שיש ביניהם מערכת יחסים רומנטית. 2. מיסרור בעל אופי מיני בין שותפים החולקים את המסרור מחוץ למערכת היחסים. 3. מיסרור בין אנשים שאינם במערכת יחסים עדיין, אך אחד מהם לפחות קיווה להיות במערכת כזו עם האחר.

מה החשש?

- הילד ייחשף לתכנים שאינם תואמי גיל
- המסר או התמונה יכולים להמשיך ולהתגלגל הלאה ברשת
- הילד ייפגע או יפגע באחר בלי משים

מה ניתן לעשות?

מה ניתן לעשות?

- לשוחח עם הילד על הקלות של הפצה ברשת ובעיקר בטלפונים ניידים ובעיקר לדון בהשלכות של העברת מסרים מיניים ברשת.
- להסביר שיש פרטים אישיים שעדיף לא לתעד בטלפון נייד מחשש שהדבר יעבור לאחר אף בשוגג
- לציין שוב ושוב בפני הילדים את ההשפעה של הפצת מידע פרטי
- להסביר לילדים מהם שירותים מבוססי מיקום מתי כדאי להשתמש בהם ומתי זה אינו רצוי
- להגדיר בטלפון הנייד איזה אפליקציות יעשו שימוש [בשירותים מבוססי מיקום](#) ואיזה לא.

אם את חברה שלי - תגלי לי את הסיסמה שלך

ילדים צעירים נוטים למסור את סיסמאות החשבונות שלהם במחשב בקלות כאות לאמון וחברות. הם עדיין לא מבינים את ההשלכות למסירת הסיסמה ולרוב לא בוחרים סיסמה בטוחה. **כדי שסיסמה תהיה "חזקה" היא צריכה להיות קשה לניחוש - מה עושים?**

- אל תשתמשו בסיסמה 12345 או ההפך 54321. זה נפוץ וקל לפריצה
 - אל תשתמשו בכל פרט הקשור בביוגרפיה שלנו כסיסמה.
- למשל: תעודת זהות, תאריך לידה, מס נייד או טלפון, שמות ילדים, שם פרטי שלך ושם משפחה וכ"ו. אלה הפרטים הראשונים שהאקר יחפש על מנת לפרוץ באמצעותם.
- אל תשתמשו באותה סיסמה בכל האתרים שלך. מי שפרץ לאחד מהאתרים שלך, ינסה באותה סיסמה להיכנס לשאר המרחבים שלך.
 - אין לסמוך על אתרים שקוראים לעצמם אתרים מאובטחים. ראו פרק בנושא כיצד לזהות [אתר מאובטח](#).
 - ישנם אתרים שמציעים לגולש "שמירת סיסמאות" – שימו לב, אל תשמרו סיסמאות באתרים אלו. לעתים קרובות הם נבנו ע"י האקרים לצורך פריצה.

אז מה כן?

- חשבו על מילה בעברית וכתבו אותה על פי המקלדת באנגלית. למשל: צאלון MTKUI
- ערבבו אותיות ומילים באותה שיטה שלמעלה.
- השתמשו במשפטים מהתנ"ך או ממערכונים למשל: "זה לא קשה זה צמיגי"
- קחו את האות הראשונה של כל מילה ועל פי המקלדת הפכו אותה לאנגלית

ז- Z, ל- K, ק- E וכך הלאה...

והרי סיסמה שלא ניתנת לפריצה.

את הסיסמאות כדאי לכתוב על נייר ולשמור במגירה, שמירת סיסמאות במחשב, זה כמו לנעול את הבית במפתח ולהשאיר את המפתח מתחת לשטיח. כולם יודעים שהוא שם..

אינסטגרם, WhatsApp....

קיים שימוש הולך וגובר באפליקציות לשם תקשורת ושיתוף. הנפוצות ביניהן: אינסטגרם שהינו יישום מאפשר למשתמש לצלם תמונות ולאחר מכן לשתף אותן ברשתות חברתיות וכן "לעקוב" אחרי משתמשים אחרים באמצעות הרשת החברתית של אינסטגרם, שם ניתן לצפות ולהגיב על תמונות של אחרים. היישום מאפשר הוספה של מסננים גרפיים שונים המשדרגים את חזות התמונות ומעניקים להן מראה שונה.

באפליקציית האינסטגרם קיימת אפשרות אם להצמיד מיקום גיאוגרפי לכל תמונה או לא. האופציה לתייג מיקום ניתנת בכל פעם שמפורסמת תמונה וניתן להגדיר שלא לצרף מיקום. בנוסף, ברירת המחדל הינה שהתמונות המצולמות פתוחות לכל העולם – שינוי בהגדרות יהפוך את התמונות לנראות רק עבור החברים.

חשוב לשוחח עם ילדיכם אודות פרטיות. לכל משפחה אמות מידה שונות לגבי הגדרת הפרטיות בביתה. שימוש באפליקציות מסוג זה יאפשרו חשיפה לתכנים שונים לכן חשוב לקבוע ביניכם כללים אלו תמונות ראוי להעלות לרשת וממה להימנע.

אפליקציה נוספת שנמצאת בשימוש נרחב היא ווטסאפ (WhatsApp) בהסתכלות ראשונית אפליקציה זו נראית כמו מערכת מסרונים, אך ההבדל המשמעותי הוא ביכולת ליצור קבוצות משמשים ולהעביר להם כקבוצה העברת הודעות טקסט, תמונות, וידאו ליחיד ולקבוצה תוך הגדרת מיקום התמונה והמשתמש(מסרון שנשלח לקבוצה מגיע לכל המשתמשים ששייכים לה והם כמובן יכולים להעביר זאת הלאה בקלות...). קלות הפצת המידע מחייבת הפעלת שיקול דעת מה להעביר ובמי לבטוח... שוחחו עם ילדיכם על הקלות בה תמונה מופצת ומה ההשלכות לכך.

יש דרכים להישמר מקרינה

חיינו סובבים מכשירים אלקטרוניים שונים המשפרים את איכות חיינו אך עלולים להוות סכנה כמקור קרינה ולהשפיע על בריאותנו. מהי בעצם קרינה?

האם יש קרינה מהמכשירים האלקטרוניים האישיים בהם אנו משתמשים כיצד ניתן להפחית את עוצמת הקרינה כלפינו?

העלאת המודעות לשימוש נכון בטלפונים ניידים, טאבלטים ומחשבים ניידים. אבחנה מתי הקרינה גבוהה יותר (בעת הורדת האפליקציות) וניסוח כללי בטיחות לשימוש מושכל. חוזר מנכ"ל¹¹ מספר 2.2-73 מרחיב ומספק המלצות למחנכים והורים

בואו נדבר על זה – כיצד הילדים יכולים לשמור על עצמם?

- הרחקת הטלפון הנייד בזמן שלא מדברים איתו מהגוף (כולל שעות הלילה) ושימוש באוזניים
- קיצור משך השיחה והעדפת שליחת מסרון על פי שיחה
- כאשר מורידים אפליקציות, כדאי להניח את הטלפון הנייד במרחק ולחזור אליו לאחר ההורדה
- לא לשבת עם המחשב ישירות על הגוף אלא להניח על שולחן מרוחק מרחק סביר (מרחב עבודה)
- לשים לב לכתבות בתקשורת בנושא ולפעול על פי הנחיות המשרד להגנת הסביבה

¹¹ <http://cms.education.gov.il/EducationCMS/Applications/Mankal/EtsMedorim/2/2-2/HoraotKeva/K-2012-1b-2-2-73.htm>

לאן ולמי פונים

משרד החינוך

[פניות ותלונות הציבור וקו פתוח לתלמידים](#)

מוקד שירות חינוך: 1-800-25-00-25 קו פתוח לתלמידים: 1-800-222-003
www.facebook.com/MadaTech.SafeInternet בדף הפייסבוק: אתיקה ומוגנות ברשת

על אירוע באינטרנט [ובטופס הדיווח](#)

המשרד לביטחון הפנים

הפנייה דרך רכזי מצילה ו/או מנהלי תכניות "עיר ללא אלימות" ביישובים
www.cww.gov.il ; www.mezila.mops.gov.il כתובת אתר האינטרנט

איגוד האינטרנט הישראלי

www.safe.org.il, "פורטל גלישה בטוחה" [יותר חכמים מהאינטרנט](#)
מידע ותמיכה לילדים, נוער, מחנכים והורים לגלישה בטוחה ברשת.
safe@isoc.org.il קו תמיכה לפנייה ודיווח על פגיעה/הטרדה באינטרנט בטלפון: 03-9700911 במייל

ער"ן

גמורה על סודיות ועל אנונימיות נפשית עם הקפדה שירות המציע עזרה ראשונה
טלפון 24 שעות במספר: 1201
שמספרו: ICQ 12010
www.eran.org.il שיחות צ'אט ומשלוח מיילים דרך אתר ער"ן
שרות הצ'אט זמין בין השעות 16:00 אחה"צ – 02:00 בלילה
מיילים מקבלים מענה עד 24 שעות מיום השליחה

[Y elem](#)

פורטל המידע, הייעוץ והתמיכה לנוער וצעירים, שפועלים בו אנשי מקצוע מתנדבים למטרת ייעוץ ותמיכה
[צ'אט, פורום ודוא"ל](#)

www.yelem.org.il כתובת אתר האינטרנט

סַהַר

סיוע והקשבה ברשת – תמיכה נפשית

שמספרו: ICQ 179201498

www.sahar.org.il צ'אט אישי באתר

sahar.help@gmail.com בדואר אלקטרוני:

אלי

אגודה להגנת הילד, עמותה הפועלת לסיוע לילדים הסובלים מהתעללות פיזית, מינית רגשית והזנח.

בטלפון חינם שמספרו: 1-800-22-3966

www.eli.org.il כתובת אתר האינטרנט

hotline@eli.org.il בדואר אלקטרוני:

המועצה לשלום הילד

גוף הפועל לטיפול בהגנה על שלומם, רווחתם, זכויותיהם של כלל הילדים בישראל.

בטלפון שמספרו: 02-6780606, פקס: 02-679-0606

ncc@children.org.il בדואר אלקטרוני:

מקורות

התמונות המשולבות במסמך זה הינן Public Domain ונלקחו מאתר [/http://pixabay.com](http://pixabay.com)

הררי, ל', וידיסלבסקי, מ' ושמש, ד' (2011). [הדרך אל מרחב בטוח](#) – ארבעת המ"מ, אגף לחינוך יסודי

Kowalski, R. M., Limber, S. P., & Agatston, P. W. (2008). Cyber bullying: Bullying in the digital age. Oxford, UK: Blackwell.

Schiller, J. and Voisard, A., 2004. Location-Based Services. Morgan Kaufmann, 2004

Pew (2011). Americans and Text Messaging. <http://pewinternet.org/Reports/2011/Cell-Phone-Texting-2011.aspx>