משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

מדריך פרטיות תלמידים במוסדות חינוך בעידן הדיגיטלי

נובמבר 2021

In a digital age in which children's every communication and action is tracked and recorded, it is becoming clear that privacy is vital to children's "best interests" and their opportunity to develop to their full potential.

Sonia Livingstone, professor of Social Psychology and former
head of the Department of Media and Communications
at the London School of Economics and Political Science

בעידן דיגיטלי שבו כל תקשורת ופעולה של ילדים מנוטרת ומתועדת, הולך ומתבהר שפרטיות היא חיונית ל'טובת הילדים' ולהזדמנות שלהם להתפתח למלוא הפוטנציאל שלהם.

סוניה ליווינגסטון, פרופסור לפסיכולוגיה חברתית ולשעבר ראש
המחלקה למדיה ותקשורת בבית הספר לכלכלה ומדע המדינה של לונדון

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

מדריך פרטיות תלמידים במוסדות חינוך בעידן הדיגיטלי

עבור מנהלי מוסדות חינוך, מנהלי מחלקות חינוך ברשויות מקומיות ובעלויות על מוסדות חינוך

נובמבר 2021

073-3928555 | PPA@justice.gov.il | WWW.GO.GOV.IL/PPA

קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | חפשו אותנו גם בפייסבוק

תוכן עניינים

תקציר

בשנים האחרונות גובר השימוש של גני ילדים ובתי ספר בטכנולוגיות מידע. מצב זה טומן בחובו יתרונות רבים, אך מהווה גם אתגר משמעותי בכל הנוגע להגנה על פרטיות ילדים במערכת החינוך.

במדריך זה מבקשת הרשות להגנת הפרטיות במשרד המשפטים להגדיר את האתגרים והסיכונים השונים לפרטיות תלמידות ותלמידים בבתי הספר ובגני הילדים בעידן הדיגיטלי, ולהציע המלצות לשמירה ולהגנה על פרטיותם של ילדים. כמו כן, המדריך מבקש להנגיש את הוראות הדין ואת העקרונות המרכזיים בכל הנוגע לפרטיות ילדים במערכת החינוך, ולהציג מספר עקרונות להגנה על פרטיות בעת הטמעת טכנולוגיות חדשות ומתפתחות במוסדות חינוך.

המדריך מתמקד במספר נושאים מרכזיים, ובהם: החובות החלות בחוק על בעל מאגר מידע ביחס לאיסוף ושימוש במידע אישי; החובות המוטלות על מנהל מוסד חינוכי בנושאי פרטיות במידע על אודות תלמידים; טכנולוגיות מעקב הפועלות בשטח המוסד החינוכי; שימוש מוסדות חינוך במערכות לניהול פדגוגי המאפשרות להורים ולתלמידים גישה למידע על אודות תלמידים; היבטי פרטיות והגנת מידע בלמידה מרחוק; שימוש באמצעים דיגיטליים שאינם ייעודיים; והגנה על פרטיות באמצעי קצה.

המדריך מבקש לעסוק בסוגיות האמורות, הן מתוך התייחסות למצב מערכת החינוך כיום, והן מתוך ראייה צופה פני עתיד, כלומר מתוך הסתכלות על טכנולוגיות בעלות פוטנציאל לפגיעה בפרטיות, העשויות למצוא את דרכן למערכת החינוך בשנים הקרובות.

דגשים והמלצות עיקריות

- המדריך מדגיש את הצורך והחובה לשמור על פרטיות תלמידים ועל מידע הנוגע אליהם. המדריך מדגיש גם כי השימוש במידע על אודות תלמידים צריך להיעשות רק בהתאם להוראות הדין ולצורך המטרה שלשמה נאסף.
- המדריך מבקש להבהיר כי ככלל, וגם מתוך העולה מהנחיות משרד החינוך, מאגרי המידע של מוסדות חינוך רשמיים, לרבות מאגרי מידע שנוצרו על-ידי מוסדות החינוך ושמנוהלים על-ידם באופן יומיומי, נמצאים בבעלות משרד החינוך. בנוגע למוסדות חינוך לא רשמיים – בעלי המוסדות (קרי, הרשויות המקומית, רשתות החינוך ועוד) הם הבעלים של מאגרי

המידע.[1] מידע על אודות תלמידים יכול להישמר גם במאגרים של גורמים המספקים שירותים למוסדות חינוך. לדוגמה, חברה פרטית המספקת שירותי בריאות ועזרה ראשונה לתלמידים במוסדות חינוך עשויה לשמור מידע על אודות תלמידים שטופלו על-ידה במאגר מידע שמוחזק על ידה.[2]

- המדריך מפרט שורה של כללים שמקורם בהוראות דיני הגנת הפרטיות, החלים על בעלי מאגרי מידע, ושמטרתם להבטיח את ההגנה על המידע מפני שימוש שלא למטרה לשמה נאסף, ולצמצם את אפשרות זליגתו. כך לדוגמה, המדריך מציין שבעל המאגר מחויב לבצע מיפוי של מערכות המאגר הנמצאות בבעלותו או בהחזקתו; לערוך סקר סיכונים; להגן באופן פיזי על תשתיות החומרה המשמשות את המאגר; ולהקפיד על מניעת זליגת מידע בעת שימוש בהתקנים ניידים.

- המדריך מבהיר כי על פי הנחיות משרד החינוך, מנהל המוסד החינוכי הוא האחראי על יישום כללי אבטחת המידע במוסד החינוכי, שחלקם מפורטים בהמשך.

- המדריך מדגיש, בין היתר, כי על פי הנחיות משרד החינוך, על מנהל המוסד החינוכי לוודא כי מידע על אודות תלמידים המוגן על פי חוק הגנת הפרטיות, התשמ"א-1981 (להלן: 'חוק הגנת הפרטיות') - כגון נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו,[3] יישמר אך ורק במערכות ספציפיות.[4]

1 | ראו חוזר מנכ"ל "מאגרי מידע בבתי ספר – רישום, דיווח ואבטחת מידע", תש"ע/3(א), https://cms.education.gov.il/EducationCMS/Applications/Mankal/EtsMedorim/3/3-6/HoraotKeva/. החוזר קובע כי רישום מאגרים של מוסדות חינוך רשמיים מוטל על משרד החינוך. בתי הספר שאינם רשמיים (מוכרים שאינם רשמיים ומוסדות פטור) מצויים בבעלות גופים שונים (לרבות עמותות וגופים פרטיים שונים), ועל כן חובת הרישום של מאגרי המידע שברשותם חלה עליהם. בעניין זה יצוין כי על פי סעיף 8(ג) לחוק הגנת הפרטיות, התשמ"א-1981, חובת רישום מאגר מוטלת על בעל המאגר.

2 | ככלל, מעמדם של ספקי משנה הוא של מחזיקי מאגר ולא בעלי מאגר. עם זאת, הגדרת בעל ומחזיק מאגר עשויה להשתנות בהתאם לנסיבות הפרטניות של כל מקרה ומקרה.

3 | לפירוט עמדת הרשות להגנת הפרטיות בנושא הגדרת "מידע" על-פי חוק הגנת הפרטיות, ראו מסמך "גילוי דעת: מהם 'מידע' ו'ידיעה על ענייניו הפרטיים של אדם' בחוק הגנת הפרטיות", https://www.gov.il/BlobFolder/rfp/information_definition_public_hearing/he/information_privacy_law_publichearing.pdf.

4 | מערכות משרד החינוך; מוצרים חינוכיים טכנולוגיים המאושרים על ידי משרד החינוך; ספריות רשת ייעודיות בשרת בית הספר; סביבות ענן בית ספריות מסוג Microsoft Office 365 for Education. להרחבה בנושא זה ראו: מסמך מטעם משרד החינוך בנושא "מדיניות שמירה וטיפול במידע מוגן במוסדות חינוך", https://sites.education.gov.il/cloud/home/havtachat_mida/Documents/mediniyut_shmira_vetipul_bemeyda_mugan_bemosadot.pdf.

- המדריך מפרט את הכללים המרכזיים ביחס לשימוש במצלמות מעקב בשטח המוסד החינוכי. בנוגע לטכנולוגיות נוספות וחדשות למעקב אחר תלמידים – עמדת הרשות להגנת הפרטיות, כמפורט בהרחבה במדריך, היא שעל מוסדות חינוך להימנע משימוש בטכנולוגיות אלו, וכי שימוש שכזה צריך להיעשות, אם בכלל, רק לאחר קבלת אישור מטעם הגורמים הרלוונטיים במשרד החינוך, ורק לאחר שגורמים אלו בחנו את הצורך בהן ואת החלופות האפשריות להן.

- המדריך מציין את החשיבות של ניסוח הנחיות ביחס לשימוש מוסדות חינוך במערכות לניהול פדגוגי, ובמיוחד כאלו המאפשרות להורים ולתלמידים גישה מרחוק למידע. המדריך ממליץ כי עובדי הוראה המשתמשים במערכות האמורות יונחו לשקול בכובד ראש את סוג ואופי המידע אותו הם שומרים ומעלים למערכות, וזאת, בין היתר, מתוך החשש כי מידע שכזה עלול לזלוג ולהיחשף ברבים. לגישת המדריך, מומלץ כי מידע העשוי להתפרש כמידע רגיש (או כזה הניתן להסיק ממנו פרט רגיש על אודות תלמיד) לא יישמר במערכות המאפשרות להורים ולתלמידים גישה מרחוק למידע, אלא בהסכמת הורי התלמיד.

- המדריך מציין, מתוך הנחיות משרד החינוך, כי מוסדות חינוך צריכים להימנע מלהעביר מידע רגיש על אודות תלמידים באמצעים שאינם ייעודיים לכך, כגון חשבונות דוא"ל פרטיים או אפליקציות מסחריות להעברת מסרים מידיים, ולהשתמש אך ורק בכלים אשר אושרו על ידי המשרד. כמו כן, המדריך ממליץ לכלל הגורמים במערכת החינוך להימנע ככל האפשר משימוש באמצעים דיגיטליים שאינם ייעודיים להעברת מידע להורים ולתלמידים. לגישת המדריך, בנסיבות בהן לא קיימת חלופה סבירה להעברת מידע (שאינו רגיש) אלא באמצעים שאינם ייעודים, ובמידה שהדבר אינו סותר את הנחיות משרד החינוך – מומלץ לקבל את הסכמת הורים להעברת המידע באמצעים אלו.

- המדריך מפרט את עמדת הרשות להגנת הפרטיות לפיה יש מקום להסדיר את נושא זכותם של הורים לעיין במידע הנוגע לילדיהם ולתקנו, וכן להעמיד זכות זו גם לתלמיד עצמו, וזאת בכפוף למגבלות שונות כגון סוג ורגישות המידע, גילו ובגרותו של התלמיד וכדומה. ככלל, הרשות ממליצה גם לפעול לשיתוף ולמעורבות ילדים ובני נוער בתהליכי קבלת החלטות במוסדות חינוך אשר עשויה להיות להן השפעה על פרטיותם.

מדריך זה מוגש כמידע כללי לשירות הציבור ולבעלי תפקידים במוסדות חינוך ובגורמים שמוסדות אלו נמצאים בבעלותם. **הנוסח המחייב הוא הוראות חוק הגנת הפרטיות, התקנות שהותקנו מכוחו, חוזרי מנכ"ל משרד החינוך והנחיות הרשות להגנת הפרטיות.**

הדוגמאות במדריך זה הובאו כהמחשה כללית בלבד ומציגות אפשרויות ליישום התוכן המובא במדריך. הדוגמאות אינן מתאימות כפי שהן לכל מקרה, ויש לבחון כל מקרה לגופו וליישם את הוראות החוק בהתאם.

בכל מקום בו מופיעה פנייה בלשון זכר או נקבה, הכוונה היא לפנייה לכלל המגדרים.

בכל מקום בו מופיעה התייחסות להורים הכוונה היא גם לאפוטרופוסים חוקיים שנקבעו לילדים.

מוסדות חינוך – שם כולל למוסדות המספקים שירותי חינוך לילדים בגילאי לימוד חובה (ככלל, גיל שלוש עד שמונה עשרה), לרבות מוסדות של החינוך הרשמי, החינוך המוכר שאינו רשמי ומוסדות פטור, כהגדרתם בהוראות הדין, של כלל זרמי החינוך (ממלכתי, ממלכתי-דתי, משלב), ומוסדות החינוך המיוחד.

תלמידים – לרבות ילדים בגני ילדים לגילאי טרום- טרום חובה ומעלה (ככלל, גיל שלוש עד שש).

בעלויות על מוסדות חינוך – שם כולל לגורמים שמוסדות חינוך מצויים בבעלותם, לרבות משרד החינוך, רשויות מקומיות, רשתות חינוך ועמותות.

פרק א' | הקדמה

ההתפתחויות הטכנולוגיות השונות ומהפכת המידע, משפיעות על כל תחום בחיינו. השימוש הגובר באמצעים טכנולוגיים, המבקש לשפר את יעילותם של שירותים שונים ולהפוך אותם לחכמים, מתרחש בכל הספרות (spheres) המרכזיות בחברה המודרנית, לרבות הספרה הציבורית והפרטית.

תחום החינוך אינו שונה. בשנים האחרונות מספר הולך וגדל של מוסדות חינוך בארץ ובעולם – גנים ובתי ספר – משתמשים באמצעים טכנולוגיים ובטכנולוגיות מידע ותקשורת (Information and Communication Technology – ICT), וזאת לצרכים רבים ולמטרות שונות: ממצלמות במעגל סגור (CCTV) ומערכות ביומטריות למעקב ולפיקוח אחר התנהלות תלמידים בשטח מוסד החינוך (שנועדו, בין היתר, לצרכי מוגנות כל באי המוסד החינוכי), דרך מערכות לניהול פדגוגי ולניהול למידה במוסדות חינוך, וכלה בהוראה והעברת תכני לימוד "מרחוק" באמצעות אמצעי קצה וסביבות לימודיות מבוססות ענן.

לשימוש של מוסדות חינוך בטכנולוגיות מעקב, מידע ותקשורת יתרונות רבים. כך, בין היתר, טכנולוגיות אלו עשויות להביא להנגשת מידע לתלמידים ולשיפור חווית הלמידה, לייעול המעקב של מוסדות החינוך אחר ההתפתחות הלימודית של תלמידיהם, לתרום לקידום שוויון ההזדמנויות בחינוך וכן להביא לשיפור הקשר והעברת המידע בין הורים למוסדות החינוך וצוותי ההוראה.

עם זאת, השימוש ההולך וגובר של מוסדות חינוך בטכנולוגיות מעקב, מידע ותקשורת, על אף היתרונות השונים הגלומים בו, טומן בחובו גם אתגר גדול בכל הנוגע להגנה על פרטיות תלמידים וילדי גן במערכת החינוך של המאה ה-21.

כך, באופן כללי, שימוש בתי ספר בטכנולוגיות מבוססות מידע למעקב אחר תלמידים וליישום מטרות שונות של מוסדות החינוך, לרבות מטרות לימודיות, עלול לפגוע בפרטיות תלמידים בשלושה היבטים מרכזיים: ראשית, מבחינת תחושת המעקב התמידי של תלמידים והפגיעה בפרטיותם הנובעת מכך; שנית, מבחינת איסוף המידע, אגירתו במאגרי מידע בית-ספריים ומאגרים של חברות פרטיות, והשימוש בו למטרות שונות, אשר עשויים להביא ליצירת "טביעת רגל דיגיטלית" של ילדים ובכך להשפיע על עתידם; ושלישית, מבחינת חשיפתו של המידע לגורמים שונים, לרבות ברשת.

בהינתן יתרונות וסיכונים משמעותיים אלו, אימוץ של טכנולוגיות מעקב כמו גם טכנולוגית מידע ותקשורת על-ידי מוסדות חינוך בישראל, מעלה, בין היתר, את השאלות: מהם הכללים והעקרונות לאורם על מוסדות חינוך להשתמש בטכנולוגיות האמורות, וכיצד על מוסדות חינוך להשתמש בטכנולוגיות תוך שמירה על פרטיות תלמידים וילדי גן.

מדריך זה מבקש לעסוק בשאלות האמורות מתוך התייחסות למצב מערכת החינוך כיום ומתוך ראייה צופה פני עתיד – קרי מתוך הסתכלות על טכנולוגיות בעלות פוטנציאל לפגיעה בפרטיות, גם אם לא מיושמות כיום, אך העשויות להיכנס למערכת החינוך בשנים הקרובות.

במטרה להגן על פרטיות תלמידים וילדי גן במערכת החינוך יש להכיר מספר עקרונות בסיסיים, וכן ליישם את העקרונות הקבועים בחוק הגנת הפרטיות ובתקנות שהותקנו מכוחו. **תפקידו של מדריך זה הוא להגדיר את הסיכונים לפרטיות תלמידים וילדי גן בעידן הדיגיטלי ולספק למוסדות חינוך ולגורמים שמוסדות אלו נמצאים בבעלותם או תחת אחריותם (כגון רשויות מקומיות ורשתות חינוך פרטיות) כלים נגישים להתמודדות עם סיכונים אלו.**[5]

מדריך זה בנוי באופן מדורג כך שיאפשר הבנה כללית באשר למערכת החינוך בעידן הדיגיטלי, מהי פרטיות ומהם האתגרים המרכזיים בתחום ההגנה על פרטיות תלמידים וילדי גן. המדרגה הראשונה כוללת הסבר מעמיק על הוראות חוק הגנת הפרטיות בדגש על איסוף ושימוש במידע אישי. השלב הבא הוא המדרגה הטכנולוגית, אשר בה מפורטים העקרונות בתכנון והפעלה של שירותים בתחום החינוך, בדגש על תכנון לפרטיות (Privacy by Design) ושקיפות. בסוף המדריך מופיע ריכוז וסיכום חוזרי המנכ"ל והנחיות משרד החינוך הרלוונטיים, באופן ישיר ועקיף, לנושא פרטיות תלמידים.

הרשות להגנת הפרטיות מקווה כי מדריך זה יממש את מטרתו – **לסייע למנהלי מוסדות חינוך וכן לגורמים שמוסדות חינוך נמצאים בבעלותם או תחת אחריותם (כגון רשויות מקומיות ורשתות חינוך) להבהיר את הדרך לאיסוף, עיבוד ושימוש במידע במערכת החינוך לקידום מטרות חינוכיות ופדגוגיות, תוך שמירה על פרטיות תלמידים והגנה על מידע הנוגע אליהם.** נדגיש כי לאור ההתפתחויות הטכנולוגיות המתמידות, הרשות להגנת הפרטיות עשויה לעדכן מסמך זה מעת לעת בין היתר בהתאם לשינויים בנהלי והנחיות משרד החינוך.

5 | לפי סעיף 7 (ב) לחוק לימוד חובה, התש"ט-1949 (להלן: "חוק לימוד חובה") האחריות על קיום מוסדות חינוך רשמיים מוטל על משרד החינוך והרשות המקומית בה פועל המוסד, במשותף. **יובהר כי לאורך המדריך, בכל מקום בו נכתב "מוסדות חינוך ובעליהם", הכוונה היא גם לגורמים שמוסדות החינוך מצויים תחת אחריותם, כגון הרשות המקומית שבתחומה שוכן המוסד.**

הרשות להגנת הפרטיות

הרשות להגנת הפרטיות (להלן גם: "הרשות") הינה הגוף המסדיר, המפקח והאוכף את הוראות חוק הגנת הפרטיות על כלל הגופים בישראל - פרטיים, עסקיים או ציבוריים, המחזיקים או מעבדים מידע אישי באופן דיגיטלי.

במסגרת תפקידה כרגולטור של דיני הגנת הפרטיות ודיני הגנת המידע, הרשות להגנת הפרטיות מופקדת על הגנת המידע האישי המוחזק במאגרי מידע כהגדרתם בחוק הגנת הפרטיות ועל ביצורה של הזכות לפרטיות. הרשות פועלת להשגת מטרה זו באמצעות התוויית מדיניות, אסדרה, הסברה והדרכה, אכיפה מנהלית, אכיפה פלילית ופיקוחי רוחב (Audit).

הרשות להגנת הפרטיות היא שמתווה את מדיניות ההגנה על המידע האישי במאגרי מידע דיגיטליים. משימותיה המרכזיות של הרשות הן קידום שליטת הפרט במידע אישי על אודותיו, השפעה על תהליכי "עיצוב לפרטיות" בארגונים ובמערכות מידע בכל מגזרי המשק, והגברת תחושת המוגנות ותחושת הביטחון של הציבור ביחס למידע האישי המוחזק במאגרי המידע. כל זאת, במטרה לצמצם את הסיכונים הגוברים לפגיעה בפרטיות בעת החזקת מידע דיגיטלי, בעיבודו או בניהולו, והכל תוך איזון ומתן משקל ראוי לחידושים הטכנולוגים וליתרונותיהם עבור השוק, קהל המשתמשים והציבור בכללותו.

הרשות להגנת הפרטיות רואה כמשימתה העיקרית קידום של ציות לדיני הגנת המידע בכל ארגון, עסק וגוף פרטי או ציבורי המחזיקים במידע אישי, כך שיפעלו לניהול תקין של המידע שברשותם בהתאם לדיני הגנת הפרטיות. משימה עיקרית נוספת היא העלאת המודעות לזכות לפרטיות ולהגנה על מידע אישי בקרב הציבור כולו.

פרק ב' | מערכת החינוך הישראלית בעידן הדיגיטלי

מערכת החינוך מצויה מזה מספר שנים בהליכים של שינוי והתאמה לעידן הדיגיטלי. תהליכים אלו מתרחשים במספר מישורים שונים בתוך מערכת החינוך – החל מתכני הלימוד, עובר באסטרטגיות ההוראה ואופן הלמידה, וכלה ברמת ניהול המערכת הבית-ספרית ובאיסוף מידע על אודות תלמידים בצורה דיגיטלית. המטרות העיקריות של התהליכים האמורים הן, בין היתר, להתאים את מערכת החינוך לתמורות הטכנולוגיות המתרחשות, לייעל את התנהלות מוסדות החינוך לרבות בכל הנוגע למעקב אחר הישגי תלמידים ואופן התנהלותם, לשפר את הקשר עם הורים, וכן להקנות לתלמידים את הכישורים הנדרשים לחיים במאה ה-21.

תהליכים אלו כרוכים בשימוש הולך וגובר של מוסדות חינוך בטכנולוגיות מידע ואמצעים דיגיטליים שונים, שחלקם ייעודיים למטרות חינוך. טכנולוגיות אלו מוגדרות, בין היתר, כ- Educational Technology או Edtech.

במערכת החינוך הישראלית לומדים, נכון למועד כתיבת שורות אלו, כ- 2.4 מיליון תלמידים בלמעלה מ-5,200 בתי ספר ובכ- 20,000 גני ילדים. לאור האמור, וכתוצאה מהשימוש הנרחב של מוסדות חינוך בטכנולוגיות מידע ואמצעים דיגיטליים, מידע דיגיטלי רב על אודות תלמידים נאסף ונשמר במאגרי מידע שונים. מידע זה הינו מידע כגון פרטי התלמיד (שם התלמיד, שמות הורים, פרטי קשר); מאפייני התלמיד (רקע משפחתי, צרכים מיוחדים), הערכה והסמכה (ציונים שנתיים, ציוני בחינות בגרות, זכאות לתעודת בגרות); היבטים תפקודיים (נוכחות, משמעת, מעורבות חברתית), מידע הנאסף במסגרת תהליכי הלמידה מרחוק (צילום התלמיד, נתונים בדבר מקום הימצאותו ואמצעי הלימוד שברשותו, מבחני הבית שהגיש), ועוד.

מידע על אודות תלמידים נשמר במאגרי מידע הנמצאים בבעלות גורמים שונים. **ככלל, מאגרי המידע של מוסדות החינוך הרשמיים נמצאים בבעלות משרד החינוך, לרבות מאגרי מידע שנוצרו על-ידי מוסדות החינוך ואשר מנוהלים על-ידם באופן יומיומי. בנוגע למוסדות חינוך לא רשמיים – בעלי המוסדות מהווים גם הבעלים של מאגרי המידע. תחת קבוצה זו ניתן למנות את הרשויות המקומית, רשתות החינוך ועוד.**

מאגרי מידע על אודות תלמידים ניתנים לחלוקה לשלושה סוגים מרכזיים:[6]

מאגרי מידע בניהול בעלויות – מאגרי מידע הנמצאים תחת ניהול בעליהם של מוסדות החינוך (משרד החינוך, רשויות מקומיות, רשתות חינוך ועוד). כך לדוגמה, מאגר המנב"ס (מערכת ניהול בתי ספר) הנמצא תחת ניהול משרד החינוך. דוגמאות אחרות הם מאגרי מידע המרכזים נתונים כגון נתוני הסעות תלמידים ופירוט תשלומי ההורים ששולמו עבור תלמידים, הנמצאים תחת ניהול רשויות מקומיות או רשתות חינוך.

מאגרי מידע מקומיים/פנימיים – מאגרי מידע הנוצרים על-ידי מוסדות החינוך ונמצאים תחת ניהול ישיר ויומיומי של מנהלי מוסדות החינוך או גורמים הפועלים מטעמם. מאגרים אלו כוללים מאגרי מידע המכילים רשימות תלמידים שננקטו לגביהם פעולות חינוכיות שונות, רשימות תלמידים בעלי בעיות אישיות, משפחתיות או כלכליות, צרכים מיוחדים ועוד.

מאגרי מידע בניהול חברות פרטיות, ספקי משנה וארגוני מגזר שלישי – מאגרי מידע הנמצאים תחת ניהול חברות פרטיות, ספקי משנה וארגוני מגזר שלישי הפועלים במוסדות חינוך. מאגרים אלו נוצרים על-ידי הגורמים האמורים והמידע השמור בהם נוצר ונאסף כתוצאה מפעילותם במסגרת מוסדות החינוך. תחת הגדרה זו ניתן למצוא, לדוגמה, מאגרי מידע של עמותות מגזר שלישי המעבירות תכני לימוד במוסדות חינוך, וכתוצאה מכך אוספות מידע מסוים על תלמידים, מאגרי מידע של חברות טיולים הפועלות במערכת החינוך, וכן מאגרי מידע של חברות טכנולוגיה אשר מספקות אמצעים טכנולוגיים שונים למוסדות חינוך (החל מאמצעים פיזיים כגון מחשבים ושרתים ועד תוכנות לניהול מידע), ומעצם פעילותן אוספות מידע רב על אודות תלמידים.

מטבע הדברים, מידע רב עשוי להיאגר במסגרת יותר ממאגר מידע אחד. כמו כן, מידע על אודות תלמידים עשוי, במקרים רבים, להיות מועבר מגורם אחד לגורם אחר. להרחבה בנושא החובות המוטלות על בעלי מאגרי המידע ולהבחנה בין חובות אלו לחובות המוטלות על גורמים המחזיקים את המאגרים, ראו פרק ח' 1 למדריך זה.

מיפוי טכנולוגיות ואמצעים דיגיטליים במערכת החינוך

העידן הדיגיטלי מאופיין בשימוש הולך וגובר של מוסדות חינוך בטכנולוגיות ואמצעים דיגיטליים שונים, וזאת למגוון רב של מטרות וצרכים. להלן יפורטו סוגי הטכנולוגיות, המערכות והאמצעים העיקריים הנמצאים בשימוש מוסדות חינוך. יובהר כי לא כל מוסדות החינוך משתמשים בכלל המערכות שיוצגו להלן:

6 | חלוקה זו היא רעיונית ונועדה להצגת סוגי מאגרי המידע. החלוקה אינה נוגעת לסוגיית הבעלות במאגרי מידע.

מערכות לניהול למידה (LMS - Learning Management Systems) – מערכות ממוחשבות לניהול למידה ומרחבי לימוד מבוסס נתונים. מערכות אלו מאפשרות ניהול של תכני למידה וחומרים לימודיים (שיעורים מתוקשבים, ביצוע מטלות אישיות וקבוצתיות, מבחנים וכדומה). המערכות האמורות הופכות את תהליך ניהול הלמידה לאוטומטי והן מאפשרות, בין היתר, מעקב אחר תוצאות הלמידה של תלמידים ואחר נתונים שונים הנוגעים לתהליך הלמידה. מערכות אלו ואחרות נתונות לבחירת מוסדות החינוך והן מסופקות להם באמצעות ספקי משנה.

מערכות לניהול פדגוגי של מוסדות חינוך – מערכות אלו הן כלי עבודה מרכזי של מוסדות החינוך, המאפשרות להם לנהל באופן דיגיטלי היבטים שונים הנוגעים להתנהלות היומיומית של המוסד החינוכי. המערכות מאפשרות, בין היתר, הפקה של תעודות והזנה של נתונים על אודות תלמידים כגון ציונים, מידע בדבר מעורבות תלמידים באירועי משמעת, נתונים בדבר נוכחות תלמידים בשיעורים, ומידע בדבר התאמות לימודיות להן זכאים תלמידים. חלק ממערכות אלו מאפשרות גם גישה מרחוק של הורים ותלמידים למידע האמור. בדומה למערכות ניהול למידה, גם מערכות אלו מסופקות ברובן למוסדות חינוך באמצעות ספקי משנה.[7]

סביבת ענן לחינוך – סביבות ענן לחינוך הן סביבות דיגיטליות המאפשרות קיום של תהליכי הוראה, למידה והערכה באופן מקוון. סביבות אלו מאפשרות, בין היתר, למידה שיתופית באמצעות שיתוף קבצים, ביצוע פעילויות אינטראקטיביות וגיבוי מידע בשירותי ענן. במערכת החינוך בישראל פועלות סביבות ענן ייעודיות לחינוך של חברות גוגל ומיקרוסופט. כל אחת מחברות אלו מציעה למשתמשים בסביבות הענן שלהם אמצעים וכלים הייחודיים לה, כגון שירותי דוא"ל, יומן ואמצעים דיגיטליים נוספים.

סביבות תוכן מתוקשבות – סביבות תוכן הינן תוכנות לימודיות בנושאים שונים, הניתנות לבחירה על-ידי מוסד החינוך, ואשר מאפשרות לתלמידים לתרגל, להתנסות ולהעמיק את הלמידה הנעשית במסגרת המוסד החינוכי. הלמידה במסגרת סביבות התוכן נעשית באופן מקוון, ועל פי רוב, באופן עצמאי. סביבות אלו נתפסות כמאפשרות למידה אישית, אינטראקטיבית וחווייתית, העשויה לתרום להעמקת תהליכי הלמידה המסורתיים. סביבות התוכן מאפשרות, בין היתר, מעקב, תיעוד וניתוח הישגיהם של התלמידים ואופן התנהלותם. על פי רוב, השימוש של תלמידים בסביבות תוכן נעשה תוך הזדהות אישית.

7 | ההבחנה התיאורטית בין מערכות לניהול למידה למערכות לניהול פדגוגי אינה חד משמעית וישנן מערכות המשלבות בין הנושאים.

לשם כך תלמידים מקבלים ממוסד החינוך קוד אישי ושם משתמש, באמצעותם הם יכולים להיכנס ל"אזור האישי" שלהם בסביבת התוכן. סביבות התוכן והתכנים הנלמדים במסגרתן משתנים בהתאם לגיל התלמידים והשלב החינוכי בו הם נמצאים. בין סביבות התוכן ניתן למצוא, לדוגמה, את תוכנת "עשר אצבעות", הכוללת פעילויות ודפי עבודה בתחום המתמטיקה לגילאי בית ספר יסודי וקדם יסודי, מערכת yschool, המציעה לתלמידים שיעורים בנושאים שונים, כגון לימודי אנגלית וסינית, ואת מערכת "אופק", המסופקת למוסדות חינוך מטעם מטח (המרכז לטכנולוגיה חינוכית).

למידה מרחוק – למידה מרחוק משמעותה מסגרת של הרצאות ושיעורים מקוונים לתלמידים כאשר אלו נמצאים מחוץ למוסדות החינוך. במהלך השנים האחרונות החלה מערכת החינוך לקדם מסגרת זו כמענה לצורך ללמידה בתנאי חירום, וזאת בעיקר עבור תלמידים בחטיבות העליונות (בחטיבת הביניים ובתיכון). עם ראשית ההתמודדות עם נגיף הקורונה בישראל החלו מוסדות חינוך רבים לעשות שימוש בתוכנת זום (Zoom) להעברת שיעורים מרחוק ובאופן מקוון לתלמידים בכל השלבים החינוכיים הרשמיים, מגילאי גן ועד גילאי תיכון. תהליך למידה באמצעים וכלים דיגיטליים, כגון למידה משולבת מחשב או למידה מרחוק דרך האינטרנט, מוגדר, בין היתר, כ"למידה אלקטרונית" (E-learning) או "למידה ניידת" (M-learning). למידה מרחוק מהווה חלק מהלמידה המשולבת (היברידית), המהווה שילוב של למידה מקוונת ולמידה פרונטאלית (פנים אל פנים) בכיתה. למידה מרחוק יכולה להתקיים באופן סינכרוני שבו התלמידים והמורה מתקשרים זה עם זה באופן מקוון ובזמן אמת, או באופן א-סינכרוני, שבו פעילות הלימוד בין המורה לתלמידים מתקיימת בזמנים שונים. כך לדוגמה, בלמידה א-סינכרונית יכולים מורים להעביר לתלמידים משימות לביצוע בזמנם החופשי ובמסגרת של למידה עצמאית. לאחר סיום המשימה, התלמידים "מעלים" את התוצרים לרשת לבדיקת המורה ולהמשך תהליך הלימוד.

טכנולוגיות למעקב "פיזי" בשטח המוסד החינוכי – טכנולוגיות מעקב מאפשרות למוסדות חינוך לעקוב אחר מיקומם של תלמידים בשטח המוסד החינוכי ולוודא את זהותם בעת התנהלותם בשטח המוסד החינוכי ובכניסה אליו. השימוש בטכנולוגיות אלו נועד בעיקרו למטרות אבטחה, מוגנות וביטחון. כמו כן נודעו מקרים נקודתיים בהם נעשה שימוש בטכנולוגיות אלו לייעול מנגנוני אכיפת המשמעת במוסד החינוכי, אף שהדבר נאסר על פי הוראות חוזר המנכ"ל.[8] תחת הגדרה זו של טכנולוגיות מעקב ניתן לציין מספר שירותים/מוצרים הנמצאים בשימוש מוסדות חינוך בעולם, כגון: מצלמות אבטחה/מעקב במעגל סגור (CCTV); מערכות RFID (Radio Frequency Identification) וכן מערכות לבוש חכמות (Wearables) למעקב אחר מיקום תלמידים בשטח המוסד החינוכי; מערכות ביומטריות לזיהוי תלמידים בכניסה למוסד החינוכי או לצרכים אחרים (כגון רכישת מזון בקפיטריה הבית-ספרית); מערכות זיהוי פנים (Facial Recognition) לאכיפת אמצעי משמעת, בדיקת נוכחות וייעול הלמידה.

אמצעי קצה – אמצעי קצה הם שם כולל למחשבים השונים בהם משתמשים תלמידים ומורים במסגרת השיעורים המתוקשבים בכיתות הלימוד ולשם ביצוע מטלות פדגוגיות כגון כתיבת עבודות ושיעורי בית. מחשבים אלו עשויים להיות מחשבים נייחים (לרבות מחשבי כיתה וכיתות מחשב), מחשביים ניידים או מחשבי לוח (טאבלטים). מודל השימוש והבעלות באמצעי הקצה עשוי לנוע מגישה לפיה המחשבים הם בבעלות המוסד החינוכי/הרשות המקומית והם אינם משויכים באופן אישי לתלמידים, לגישה לפיה המחשבים נרכשים על-ידי משפחות התלמידים וכל תלמיד עושה שימוש במכשיר האישי אותו הוא מביא למוסד החינוכי מביתו (מודל BYOD – Bring Your Own Device). בגישה זו, תלמידים עשויים להשתמש באמצעי הקצה לביצוע מטלות לימודיות גם כשהם בביתם ושלא במסגרת שעות הלימודים.[9]

שימוש מוסדות חינוך באמצעי קצה מבטא חלק מיישום תוכנית התקשוב הלאומית להתאמת מערכת החינוך למאה ה-21. כך לדוגמה, בדו"ח משרד החינוך צוין בעניין זה כי: "... מכיוון שמערכת החינוך עוברת לדיגיטציה של ספרי לימוד, יש צורך בכך שלכל תלמיד יהיה מחשב ושבכל כיתה יהיו מחשב ומקרן לצוות החינוכי. המחשבים ישמשו ללמידה אישית, ללמידה בקבוצות קטנות או ללמידה בסביבות הלמידה המיועדת להרחבות בתחום סביבות למידה ספציפיות ...".[10] בישראל, כמו מרבית מדינות העולם, אמצעי הקצה מסופקים למוסדות חינוך על-ידי חברות טכנולוגיה פרטיות הזוכות במכרזים מרכזיים שעורכת המדינה או השלטון המקומי.

8 | להרחבה ראו: Lotem Perry-Hazan & Michael Birnhack The Hidden Human Rights Curriculum of Surveillance Cameras in Schools: Due Process, Privacy, and Trust, 48 (1) CAMBRIDGE JOURNAL OF EDUCATION, 47 (2018).

9 | להרחבה על סוגיית שימוש תלמידים באמצעי קצה בתקופת התמודדות עם משבר הקורונה ראו: מרכז המחקר ומידע של הכנסת "זמינות אמצעי קצה וחיבור לאינטרנט עבור ילדים לצורך למידה מרחוק" (27.7.20), https://fs.knesset.gov.il/globaldocs/MMM/3dbd13a0-0fcc-ea11-8107-00155d0aee38/2_3dbd13a0-0fcc-ea11-8107-00155d0aee38_11_16279.pdf.

10 | משרד החינוך "התאמת מערכת החינוך למאה ה-21: הקניית אוריינות מחשב ומידע CIL בבתי ספר יסודיים" 36, https://sites.education.gov.il/cloud/home/tikshuv/Documents/aknayat_oryanut_yesodi.pdf.

פרק ג' | הזכות לפרטיות - כללי

הזכות לפרטיות היא זכות יסוד חוקתית הקבועה בחוק-יסוד: כבוד האדם וחירותו (להלן: "חוק היסוד"). סעיף 7 לחוק היסוד קובע, בין השאר כי "כל אדם זכאי לפרטיות ולצנעת חייו". בהמשך, מפרט החוק מהי פגיעה בפרטיות על ידי אזכור מספר מצבים של פגיעה בפרטיות.

נוסף על מעמדה של הזכות לפרטיות כזכות יסוד חוקתית, נהנתה הזכות עוד לפני חקיקת חוק היסוד, להגנה מפורשת ונרחבת בחוק הגנת הפרטיות. חוק זה קובע רשימה של פעולות העלולות להיחשב כפגיעה בפרטיות, כגון פרסום תצלומו של אדם ברבים בנסיבות שבהן עלול הפרסום להשפילו או לבזותו וביצוע פעולות של בילוש והתחקות אחר אדם העלולים להטרידו. החוק חל הן על המגזר הציבורי והן על המגזר הפרטי, והוא קובע כי פגיעה בפרטיות מהווה עוולה אזרחית ובתנאים מסוימים אף עבירה פלילית שעונשה עד חמש שנות מאסר.

חוק הגנת הפרטיות כולל מספר עקרונות מרכזיים. עיקרון אחד הוא **עיקרון ההסכמה**, המבטא את שליטתו של הפרט במידע הנוגע אליו, ולפיו הפרט הוא האחראי ביחס לאיזה מידע הנוגע אליו ייחשף, ולמי. עיקרון זה בא לידי ביטוי, בין היתר, בסעיף 1 לחוק הגנת הפרטיות, הקובע כי "לא יפגע אדם בפרטיות של זולתו ללא הסכמתו". הכלל הוא שאין לאסוף מידע על אדם אלא אם הוא מודע לכך שמידע נאסף אודותיו, מסכים לאיסוף המידע וכן מסכים לשימושים השונים שאוסף המידע מבקש לעשות בו. על פי חוק הגנת הפרטיות, הסכמה בהקשר זה צריכה להיות "מדעת", קרי כזו הניתנת רק לאחר שאדם מבין את משמעות הסכמתו, ואת השלכותיה, ולהינתן במפורש או מכללא.

עיקרון מרכזי נוסף הוא **עיקרון צמידות המטרה**. על פי עיקרון זה, המוסדר תחת סעיפים 2 (9) ו- 8(ב) לחוק הגנת הפרטיות, שימוש במידע יכול להיעשות אך ורק בהתאם למטרה שלשמה הוא נאסף מלכתחילה. במובן זה, שימוש במידע למטרה אחרת מזו שלשמה נאסף, מהווה פגיעה בפרטיות.

הזכות לפרטיות אינה זכות מוחלטת, והפגיעה בה כפופה לעמידה במבחנים משפטיים מסוימים. תפיסה זו מוסדרת, בין היתר, בסעיף 18 לחוק הגנת הפרטיות. עם זאת, פגיעה שכזו צריכה להיעשות בהתאם לתכלית הוראות הדין ולעמוד בעקרונות הכללים של פעילות תחת סבירות ותום לב, וככל שמדובר בגופים ציבוריים, כגון עיריות ורשויות מקומיות – גם בדרישת **המידתיות**.

פרק ב' לחוק מתמקד בהגנה על מידע אישי, וקובע משטר הגנה על הזכות לפרטיות במאגרי מידע – להרחבה ראו פרק ו' למדריך זה העוסק בנושא. מכוח החוק הותקנו תקנות וצווים בעניינים שונים, ובהם תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "תקנות אבטחת מידע").

פרק ד' | פרטיות תלמידים בחקיקה ובפסיקה

הזכות לפרטיות של ילדים בדין הישראלי מוסדרת תחת מספר מקורות שונים. במישור הבין-לאומי, סעיף 16 לאמנת האו"ם בדבר זכויות הילד (1989), עליה חתומה מדינת ישראל, קובע כי ילד לא יהא נתון להתערבות שרירותית או בלתי חוקית בפרטיותו ובתכתובתו.[11] סעיף זה קובע גם כי ילדים זכאים להגנת החקיקה במדינות החתומות על האמנה, מפני התערבויות או פגיעות שכאלו. הזכות החוקתית לפרטיות עומדת לילדים במשפט הישראלי מכוח הוראות סעיף 7 לחוק יסוד: כבוד האדם וחירותו הקובע בצורה מפורשת כי "כל אדם זכאי לפרטיות ולצנעת חייו". זכות זו חלה גם על ילדים מהטעם שלזכויות המנויות בחוק היסוד לא נקבעה הגבלת גיל. מאותו הטעם גם הוראות הדין הכללי בישראל בנוגע לפרטיות, לרבות הוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו, חלות גם על ילדים, וזאת במישורים שונים של חייהם ולרבות בכובעם כתלמידים. עיקרון זה נובע גם מהוראות סעיף 12 לחוק זכויות התלמיד, התשס"א-2000 (להלן: "חוק זכויות התלמיד"), הקובע כי מוסד חינוך לא ימנע מתלמיד לממש את זכויותיו כאמור בחוק זה או בכל דין אחר.

בנוסף לתחולת ההוראות הכלליות של חוק הגנת הפרטיות, הסוגיה הספציפית של פרטיות תלמידים מוסדרת בהוראות הדין תחת סעיף 14 לחוק זכויות התלמיד, אשר קובע חובת סודיות לפיה כל אדם שהגיע אליו מידע על תלמיד עקב מילוי תפקיד שהוטל עליו לפי חוק זה, חייב לשמור המידע בסוד ולא לגלותו, אלא לצורך ביצוע תפקידו.

השימוש של בתי המשפט בסעיף 14 לחוק זכויות התלמיד מועט.[12] כך, במקרה אחד קבע בית משפט השלום בתל אביב, על יסוד הוראות סעיף 14, שמורה שפרסמה מכתב בו כללה את דעתה (השלילית) בנוגע לתלמידה מסוימת, הפרה את חובת החיסיון שהוטלה עליה מכוח חוק זכויות התלמיד.[13] במקרה אחר ביקר בית המשפט מורה אשר במסגרת תביעת לשון הרע שהגישה, צרפה נספח ובו מידע על אודות תלמידים, וזאת תוך שציין כי היה ראוי לקבל את הסכמת הורי התלמידים

11 | על פי סעיף 3 לאמנה, בהחלטות המתקבלות בנוגע לילדים צריך עיקרון טובת הילד להיות עיקרון "ראשון במעלה". עיקרון מרכזי נוסף הוא עיקרון השתתפות ילדים בהליכי קבלת החלטות המתקבלות בעניינם, אשר מוסדר בסעיף 12 לאמנה.

12 | ייתכן כמובן שהדבר נובע ממיעוט מקרים הנוגעים להפרת הוראות הסעיף אשר מגיעים בסופו של יום לבתי המשפט.

13 | ת"א (שלום ת"א) 62077-07 **אילן ישעיהו נ' אביטל עמר** (פורסם בנבו, 13.09.10). בפסק הדין נקבע שמורה שפרסמה מכתב בו כללה את דעתה (השלילית) בנוגע לתלמידה מסוימת, הפרה את חובת החיסיון שהוטלה עליה מכוח ס' 14 לחוק זכויות התלמיד.

טרם הפרסום.[14] במקרה נוסף הגביל בית הדין האזורי לעבודה בחיפה את זכות העיון של מורה במידע על אודות תלמידים, במסגרת הליך משפטי שניהלה כנגד מוסד חינוכי שבו לימדה.[15] כפי שעולה מתוך הדברים, סעיף 14 לחוק זכויות התלמיד לא זכה עד כה לפרשנות שיפוטית בכל הנוגע להפרת חובת הסודיות הקבועה בו בהקשר הרשתי, קרי ביחס להגנה על מידע דיגיטלי על אודות תלמידים.

סמכותם של מוסדות חינוך, והגורמים הפועלים במסגרתם, לפעול מבחינה חוקית תוך פגיעה בפרטיות תלמידים מוסדרת, הלכה למעשה, תחת שני הסדרים מרכזיים:

האחד, פסקת ההגבלה הקבועה בסעיף 8 לחוק יסוד כבוד האדם וחירותו, המאפשרת באמצעות חקיקה ובתנאים מסוימים לגופים ציבוריים לפעול תוך פגיעה בזכויות המוסדרות בחוק היסוד, לרבות הזכות לפרטיות. השני, סעיף 18 לחוק הגנת הפרטיות, הקובע רשימה של מקרים המצדיקים לכאורה התנהלות הפוגעת בפרטיות, והמעניקים למי שפועל בנסיבות אלו תוך פגיעה בפרטיותו של אחר הגנה במשפט אזרחי או פלילי. כך לדוגמה, סעיף 18(2)(ב) לחוק הגנת הפרטיות קובע כי במקרה בו פגיעה בפרטיותו של אדם נעשתה בתום לב ובנסיבות בהן הייתה על הפוגע "חובה חוקית, מוסרית, חברתית או מקצועית לעשותה", הרי שהפוגע יהיה מוגן מפני הסנקציות הקבועות בחוק. ובדומה, סעיף 18(3) קובע כי הגנה שכזו תעמוד במידה ובפגיעה היה עניין ציבורי המצדיק אותה בנסיבות העניין. על אף שאין מדובר בסעיף מסמיך, סעיף 18 נתפס לעיתים על-ידי מוסדות ואנשי חינוך ככזה המאפשר להם לפעול בנסיבות הכרוכות בפגיעה בפרטיות תלמידים.[16]

עד כאן החקיקה והפסיקה הרלוונטיים לסוגיית פרטיות של ילדים במערכת החינוך. יצוין כי מרבית ההיבטים הנוגעים לפרטיות תלמידים מוסדרים כיום בהוראות חוזרי מנכ"ל משרד החינוך, המסדירים היבטים שונים הנוגעים לפרטיות תלמידים במערכת החינוך, ושחלקם יפורטו בהמשך המדריך.

14 | ת"א (קריות) 25259-06-13 **עבדי נ' עומר ש.ל. תקשורת מקומית בע"מ עיתון "הד הקריות"** (פורסם בנבו, 18.4.17).

15 | פ"ה (חי') 1054-09-16 **סמעאן נ' ביה"ס פטריארכאלי לטיני – ראמה** (פורסם בנבו, 15.1.17).

16 | **בין הורים למורים בחינוך העל-יסודי – תמונת מצב והמלצות** 125 (ציפורה שכטמן ועודד בושריאן עורכים, 2015), http://education.academy.ac.il/SystemFiles/23008.pdf.

פרק ה' | פרטיות תלמידים בעידן הדיגיטלי - אתגרים מרכזיים

שימוש מוסדות חינוך במערכות טכנולוגיות שונות במסגרת הוראה, מעקב אחר התנהלות תלמידים (נוכחות, איחורים, השתתפות בלמידה וציונים), וניהול המערכת הבית-ספרית בכללותה, טומן בחובו יתרונות רבים. עם זאת, במקביל ליתרונות אלו, שימוש זה כרוך גם בפגיעה בפרטיותם של תלמידים. פגיעה זו בפרטיותם של תלמידים ניתנת לחלוקה לארבעה אתגרים מרכזיים:

מעקב אחר תלמידים

אתגר מרכזי הנוגע לפרטיות תלמידים במערכת החינוך הוא השימוש ההולך וגובר של מוסדות חינוך בטכנולוגיות מעקב (Monitoring/Surveillance) ותחושת המעקב הנוצרת בקרב תלמידים לאור שימוש שכזה.

כפי שצוין קודם לכן, מוסדות חינוך במדינות שונות בעולם עושים שימוש בטכנולוגיות מעקב מסוגים שונים, כגון מערכות ביומטריות בכניסה למוסדות חינוך, מערכות מבוססות טכנולוגיית RFID למעקב אחר מיקום תלמידים ומערכות מבוססות אינטליגנציה מלאכותית (AI) לניטור התנהלותם של תלמידים. בישראל, ככל הידוע, רק מצלמות אבטחה/מעקב נמצאות כיום תחת שימוש מוסדר ו"רשמי" של מוסדות חינוך בישראל. עם זאת, שאר טכנולוגיות המעקב שצוינו נמצאות כבר בשימוש מוסדות חינוך במדינות רבות בעולם.

ככלל, השימוש באמצעים טכנולוגיים למעקב בשטח המוסד החינוכי נועד לכאורה לשם הגנה על תלמידים ומורים, ועל רכוש מוסד החינוך. אלו מטרות ראויות. עם זאת, שימושים באמצעים כאלו יכול לנבוע גם משיקולים אחרים. כך לדוגמה, שימוש במצלמות יכול לנבוע משיקולים מערכתיים כגון שיפור יעילות הליכי הבירור במקרים של הפרות משמעת, וצמצום השימוש במורים להשגחה על תלמידים בזמן ההפסקות. על-פניו ניתן לטעון כי שימושים שכאלו, שלעצמם, אינם מצדיקים שימוש בטכנולוגיות מעקב בעלות פוטנציאל גבוה לפגיעה בפרטיות תלמידים.

בכל מקרה, תהא מטרת השימוש אשר תהא, שימוש מוסדות חינוך בטכנולוגיות האמורות עלול להביא לפגיעה קשה בפרטיותם של תלמידים. יובהר שלמיטב ידיעתנו, פרט למצלמות מעקב, שימוש בטכנולוגיות מעקב כמעט ולא מתקיים כיום במוסדות החינוך בישראל, ובכל מקרה שימוש שכזה חייב להיעשות בהתאם לדיני הגנת הפרטיות והנחיות משרד החינוך.

שימוש מוסדות חינוך בטכנולוגיות מעקב עלול ליצור בקרב תלמידים תחושה של מעקב תמידי, לפיה כל פעולה שלהם במסגרת שטח בית הספר מנוטרת, מתועדת ונאגרת – וזאת מבלי שיש בידי התלמידים האפשרות לסרב למעקב זה או למצער לצמצם את היקפו. מצב זה נתפס, ברמה העקרונית, כהפרה של פרטיות.

שימוש נרחב של מוסדות חינוך בטכנולוגיות מעקב מסוגים שונים עלול גם להרגיל ילדים למציאות של מעקב תמידי (קרי "לנרמל" עבורם מציאות שבה מעשיהם מחוץ לבית מנוטרים בכל עת), באופן שלא יראו בה כל קושי גם בבגרותם, על כל הבעיות הנובעות מכך, ועל ההשלכות החברתיות של נרמול זה.

איסוף ושימוש במידע דיגיטלי על אודות תלמידים

שימוש מוסדות חינוך בטכנולוגיות מידע מושתת ברובו על איסוף, אחסון ושימוש במידע דיגיטלי על אודות תלמידים. משמעות הדבר היא שבמהלך לימודיהם של תלמידים נאסף עליהם מידע רב, לרבות מידע אישי ומידע הנוגע להתנהלותם החברתית והישגיהם. מידע זה הנשמר במאגרי מידע, ובוודאי כזה העולה לרשת, עלול לייצר לתלמידים "טביעת רגל דיגיטלית" – אשר תלווה אותם גם בהמשך חייהם.

המידע נאסף ונשמר, בין היתר, כתוצאה משימוש תלמידים בסביבות תוכן מתוקשבות. מידע זה עשוי לכלול - בנוסף לפרטים האישיים של התלמיד - פרטים כגון מיקום התלמיד, תכנים אליהם הוא נחשף במסגרת פעילותו, או עמודים בהם ביקר ברשת. ספקי סביבות התוכן עשויים לאסוף גם נתונים סטטיסטיים וכן לעשות שימוש בקבצי "עוגיות" להתאמת סביבת התוכן ושיפור השירות. במקרים מסוימים המידע עשוי להיאסף גם לשם הצגת מודעות ממוקדות לפי תחומי העניין של התלמיד.[17]

על מוסדות החינוך לנהוג בשקיפות מלאה לעניין איסוף המידע והשימושים שהם עושים במידע על אודות תלמידים, או עשויים לעשות במידע זה, לרבות העברתו לצדדים שלישיים.

זליגת וחשיפת מידע על אודות תלמידים

שימוש מוסדות חינוך במערכות דיגיטליות הוא בלתי נמנע בימינו. כאמור, במציאות שכזו, מידע דיגיטלי רב על אודות תלמידים נאסף ונשמר במאגרי מידע. **מידע זה עלול לזלוג ולהיחשף בפני גורמים לא מורשים, ובכך לפגוע בפרטיותם של תלמידים.** זליגה וחשיפה של מידע עלולות להיגרם

17 | https://www.cet-catalogue.cet.ac.il/privacy-policy.

הן כתוצאה מפריצה מתוכננת למאגר המידע והן כתוצאה מאי-אבטחת המידע בצורה מספקת. דוגמה לדברים ניתן לראות במקרה שהתרחש בשנת 2017 במדינת מונטנה שבארצות הברית, בו נפרצו מאגרי מידע של מספר בתי ספר, תוך שהפורצים איימו לחשוף את המידע אם לא יועבר להם תשלום.[18] אירועים של זליגת מידע על אודות תלמידים התרחשו גם בישראל.[19]

זליגת מידע וחשיפה לא רצויה שלו עלולה להיגרם גם כתוצאה משימוש מוסדות חינוך בטכנולוגיות מעקב. שימוש מוסדות חינוך בטכנולוגיות מעקב מביא, בסופו של יום, לאיסוף ואגירת מידע רגיש על אודות ילדים אשר יכול לזלוג ולהגיע, בטעות או בזדון, לגופים העלולים לעשות בו שימוש לרעה. כך לדוגמה, בארה"ב פורסם על מקרה בו מצלמת אבטחה שמוקמה באזור אולם ההתעמלות של מוסד חינוכי כללה בשדה הראייה שלה גם את אזור תאי ההלבשה של התלמידים.[20] חשיפת מידע יכולה להתרחש גם כתוצאה מפריצה לאמצעי המעקב בזמן אמת.

בהקשר זה יש לזכור כי מידע הנאסף ומועבר במסגרת שימוש מוסדות חינוך במערכות תקשורת ומידע הוא במקרים רבים, מידע רגיש כהגדרתו בחוק הגנת הפרטיות (או מידע בעל רגישות באופן כללי). כך לדוגמה, מתוך מידע על התאמות לימודיות הניתנות לתלמיד ניתן בקלות ללמוד על מצב בריאותו ועל קשיים ובעיות עימם הוא מתמודד. כל האמור מחדד את הבעייתיות בזליגת ובחשיפת המידע האמור לגורמים לא מורשים.

שימוש פסול במידע על-ידי מוסדות חינוך וחברות פרטיות

חשש נוסף העולה מתוך שימוש מוסדות חינוך במערכות טכנולוגיות הוא שמוסדות חינוך, בעלי המוסדות, וכן חברות פרטיות המעניקות שירותים טכנולוגיים למוסדות אלו, ישתמשו במידע על אודות תלמידים באופן בלתי חוקי (קרי שלא למטרה שלשמה נאסף המידע מלכתחילה), לרבות תוך העברתו לצדדים שלישיים.

כך לדוגמה, בשנת 2010 קנסה הרשות להגנת הפרטיות (בשמה הקודם רמו"ט) את עיריית רמת גן בגין העברה של מידע על אודות תלמידים ממאגר מידע שבבעלותה, לחברת "קידום".

18 | Rhett Jones, Hackers Lock down Entire School District with Threats: 'We Are Savage Creatures', Gizmodo (Sep. 19, 2017), https://gizmodo.com/hackers-lock-down-entire-school-district-with-threats-1818542996

19 | מבקר המדינה, דוח שנתי 69ב (2019), בעמ' 58-59.

20 | Brannum v. Overton County Sch. Bd., 516 F.3d 489, 497 (6th Cir. 2008). יצוין כי בתקשורת מפורסמים לא פעם מקרים בהם צילומים ממצלמות אבטחה, לרבות כאלו המתעדים פרטים הנמצאים במצבים אינטימיים, זולגים ונחשפים ברשתות חברתיות.

נמצא כי העירייה הפרה את הוראות הדין בהקשר זה והוטלו עליה קנסות מינהליים בגין הפרה זו.[21] מטבע הדברים, חשש זה מתעצם שעה שחברות פרטיות רבות, שחלקן אף אינן ישראליות, מעניקות שירותים טכנולוגיים שונים למוסדות חינוך בישראל, שבמסגרתם נאסף מידע אישי רב על אודות תלמידים במאגרי המידע שלהן. חברות אלו עלולות להשתמש במידע ליצירת פרופיל של תלמידים ("פרופיילינג"), אשר עשוי לשמש אותן (בהווה ובעתיד) למטרות שונות, לרבות מטרות מסחריות.

עד כאן פירוט האתגרים המרכזיים. יובהר כי אין באמור בכדי לטעון שעל מוסדות חינוך להימנע משימוש בטכנולוגיות מידע המאושרות על-ידי משרד החינוך, אלא ששימוש זה צריך להיעשות בהתאם להוראות הדין ותוך הגנה על פרטיותם של תלמידים.

יצוין כי בין השנים 2018-2019 ערכה הרשות להגנת הפרטיות פיקוח רוחב בקרב גופים המנהלים פלטפורמות לימודיות וחינוכיות אודות קטינים. בכל הנוגע לאבטחת מידע, הליך הפיקוח מצא כי במרבית הגופים (75%) נמצאה רמת עמידה גבוהה בהוראות הדין. עם זאת, נמצאו גופים המנהלים מידע על קטינים, אשר במערכותיהם לא הותקנו אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב. ההליך מצא גם כי גופים רבים מאלו שנבדקו לא ניהלו את מאגרי המידע שלהם כנדרש. כמו כן נמצא כי בכ-80% מהגופים שנבדקו נפלו כשלים באופן עבודתם עם גורמים שלישיים אשר אליהם הם העבירו מידע על אודות קטינים. כך לדוגמה, נמצא כי גופים רבים לא בחנו את איכות ניהול אבטחת המידע בגורמים שאליהם הם העבירו את המידע ולא פעלו כנדרש לפיקוח על אופן התנהלותם של גורמים אלו. הליך הפיקוח מצא גם כי מרבית הגופים שנבדקו אינם מקפידים דיים ליידע את ציבור הקטינים על האופן שבו נאסף המידע אודותיהם, ואינם מיידעים את הקטינים בצורה מספקת בדבר זכויותיהם מכוח חוק הגנת הפרטיות, כדוגמת הזכות לעיין במידע על אודותיהם.[22]

בפרקים הבאים נציג את הדין החל והמלצות הרשות להגנת הפרטיות ביחס ליישומו.

21 | הרשות למשפט טכנולוגיה ומידע, דו"ח שנתי לשנת 2010 (28.12.11), https://www.justice.gov.il/Units/ilita/Dohot/report2010.pdf.

22 | עיון בממצאי דו"ח פיקוח הרוחב ראו: https://www.gov.il/BlobFolder/news/website_platforms_and_learning_apps/he/Minors_report.pdf.

פרק ו' | החובות הכלליות בחוק ביחס לאיסוף ולשימוש במידע אישי

פרק זה מפרט את הדרישות הבסיסיות לפי חוק הגנת הפרטיות בעניין איסוף ושימוש במידע אישי במאגרי מידע. דרישות אלה רלוונטיות הן ביחס לטכנולוגיות המשמשות את מוסדות החינוך והן ביחס למאגרי המידע הנוצרים במסגרת השימוש בטכנולוגיות האמורות.

נזכיר שוב כי כלל מאגרי המידע של מוסדות החינוך הרשמיים נמצאים בבעלות משרד החינוך, הנחשב כ"בעל מאגר המידע". בכל הנוגע למוסדות חינוך לא רשמיים – בעלי המוסדות (כגון רשויות מקומיות ורשתות חינוך) הם המהווים הבעלים של מאגרי המידע של מוסדות אלו. כפי שיפורט בהמשך, על פי הנחיות משרד החינוך, מנהלי מוסדות חינוך מוגדרים בהקשר זה כ"מנהלי המאגרים".

ניהול מאגרי מידע

כפי שצוין קודם לכן, במסגרת פעילות מוסדות חינוך **מצטברת כמות עצומה של מידע אישי על אודות תלמידים ממקורות ומאגרים שונים,** החל ממאגרים בית-ספריים פנימיים ובסיסיים המכילים מידע כללי על אודות תלמידים ועד מאגרים שנמצאים בניהול בעלויות על מוסדות חינוך. כאמור מידע על אודות תלמידים נאסף ונאגר גם על ידי גורמים חיצוניים וקבלני משנה (ספקים) המספקים שירותים למוסדות החינוך.

היקף המידע ורגישותו מחייבים את מוסדות החינוך, את הגורמים הרלוונטיים שמוסדות אלו נמצאים בבעלותם (כגון עיריות או רשתות חינוך) ואת הגופים הפרטיים הפועלים במסגרת מערכת החינוך (וכתוצאה מכך אוספים ואוגרים מידע על אודות תלמידים), לנהל את מאגרי המידע בצורה מאובטחת, תוך הקפדה על ניהול קפדני של מאגרי המידע ויישום תקנות אבטחת מידע על מנת למנוע זליגת מידע אישי או פריצה למאגרים אלה.

בפרק ב' לחוק הגנת הפרטיות, נקבעו הוראות לעניין הגנה על הפרטיות במאגר המידע, בין היתר בהיבטי חובת הרישום של מאגר המידע אצל רשם מאגרי המידע (כיום הרשות להגנת הפרטיות), אופן החזקת מאגר המידע, אבטחת מאגר המידע, חובות בעל המאגר ומנהל המאגר, זכויות נושאי המידע (יחידים שמידע על אודותיהם נאסף ונשמר במאגרי המידע) וכן השימושים המותרים במידע השמור במאגרי המידע השונים. להלן פירוט ההיבטים המרכזיים:

1. **חובת הרישום –** בהתקיים אחד התנאים בסעיף 8(ג) לחוק, נדרש בעל מאגר מידע לרשום את המאגר אצל רשם מאגרי המידע ברשות להגנת הפרטיות.
על פי הנחיות משרד החינוך, משרד החינוך הוא האחראי על רישום מאגרי מידע של מוסדות חינוך רשמיים (לרבות מאגרי מידע פנימיים הנוצרים על-ידי מוסדות החינוך). במוסדות חינוך שאינם רשמיים (מוכרים שאינם רשמיים ומוסדות פטור) חובת הרישום חלה על הגורמים שמוסדות החינוך מצויים בבעלותם.

2. **עיקרון צמידות המטרה –** על פי עיקרון זה, הגורם האוסף מידע מחויב לעשות בו שימוש אך ורק לשם המטרה שלשמה הוא נאסף מלכתחילה, ולא לשם אף מטרה אחרת (סעיף 8(ב) לחוק הגנת הפרטיות).
לדוגמה, מוסד חינוכי או גורם שהמוסד מצוי בבעלותו, הנחשפים למצב כלכלי קשה של משפחתו של תלמיד (לדוגמה לאחר שזו ביקשה הנחה בגובה תשלומי הורים ונדרשה לשם כך להציג תימוכין בדבר מצבה הכלכלי), מנועים מלהשתמש במידע האמור לכל מטרה אחרת פרט לטיפול בבקשה להנחה שבמסגרתה נחשף המידע. כל שימוש במידע למטרה אחרת עלול בהקשר זה להיחשב הפרה של הזכות לפרטיות של התלמיד ומשפחתו.
על בסיס עיקרון צמידות המטרה נדרש כי בעל מאגר המידע יימנע ככל האפשר מאיסוף מידע עודף שאינו נדרש לשם מטרת האיסוף או מאגר המידע. כמו כן, לאחר שלב איסוף המידע, על בעל המאגר לבחון האם הוא מחזיק מידע עודף שאינו נדרש לשם מטרת האיסוף או המאגר.[23]

3. **חובת מתן הודעה –** על פי עיקרון זה, כל גורם המבקש לאסוף מידע, להחזיק או להשתמש בו, מחויב ליידע את האדם נושא המידע (או את האפוטרופוס החוקי שלו – אם מדובר בקטין), בטרם איסוף המידע הנוגע אליו, האם חלה עליו חובה חוקית למסור את המידע או שמסירת המידע תלויה ברצונו והסכמתו, וכן מהי המטרה שלשמה מבוקש המידע, ולמי הוא יימסר (סעיף 11 לחוק).

4. **זכות עיון במידע –** חובת כל בעל מאגר מידע לאפשר לכל אדם לעיין במידע על אודותיו המוחזק במאגר המידע, וזאת תחת מספר מגבלות המפורטות בסעיף 13 לחוק.

23 | תקנה 2(ג) לתקנות אבטחת מידע קובעת כי "בעל מאגר מידע יבחן, אחת לשנה, אם אין המידע שהוא שומר במאגר רב מן הנדרש למטרות המאגר". יצוין כי טיוטת מסמך מקיף מטעם הרשות להגנת הפרטיות בנושא "צמצום מידע" התפרסם לקבלת הערות הציבור בנושא. לעיון במסמך ראו: https://www.gov.il/he/departments/publications/Call_for_bids/data_minimization_public_hearing.

5. **זכות תיקון המידע –** נושא המידע רשאי לדרוש תיקון של מידע על אודותיו, ככל שהמידע המצוי במאגר אינו נכון, שלם, ברור או מעודכן (סעיף 14 לחוק).

בכל הנוגע לזכויות העיון במידע על אודות תלמידים ולתיקונו – נושאים אלו אינם מוסדרים באופן כולל בהנחיות משרד החינוך, אלא רק תחת הסדרים פרטניים מסוימים. כך, לפי סעיף 6.5 ג. (2) (ט) לחוזר מנכ"ל "מאגרי מידע בבתי ספר – רישום, דיווח ואבטחת מידע", הורים זכאים לקבל מידע פרטני על בנם/בתם בלבד בו נעשה שימוש במערכות המשתמשות בבסיסי הנתונים של המנב"ס או שנשמר במאגרי מידע אחרים בבתי הספר. סעיף 2.6 לחוזר מנכ"ל "מצלמות במוסדות החינוך – הסדרת הכנסתן ואופן התקנתן", קובע כי תלמיד שתועד במצלמת מעקב המותקנת במוסד החינוך והוריו רשאים לצפות בחומרים המצולמים והנוגעים לתלמיד, וזאת בכפוף למגבלות שונות המפורטות בחוזר.

עמדת הרשות להגנת הפרטיות היא כי יש מקום להסדיר את כל נושא זכותם של הורים לעיין במידע הנוגע לילדיהם ולתקנו, וכן להעמיד זכות זו גם לתלמיד עצמו, וזאת בכפוף למגבלות שונות כגון סוג ורגישות המידע, גילו ובגרותו של התלמיד וכדומה.

6. **חובת הסודיות –** בעל מאגר המידע, הגורם המחזיק במאגר ומי מעובדיהם, מחויבים בשמירת סודיות המידע אליו נחשפו כחלק מעבודתם (סעיף 16 לחוק). כפי שצוין קודם לכן, סעיף 14 לחוק זכויות התלמיד מחיל חובה זו באופן מפורש על כל מי שפועל מכוחו ואוסר על גילוי מידע על תלמיד שהגיע אליו, אלא לצורך ביצוע תפקידו.

לדוגמה, מחנך כיתה הנחשף לכך שתלמידו מצוי במצב משפחתי מורכב, כגון גירושי הורים, מחויב שלא לחשוף את המידע שלא בהסכמת התלמיד או הוריו, אלא במצבים בהם הוא חושב שחשיפת המידע נדרשת לשם ביצוע תפקידו כמחנך ומתוך ראיית טובת התלמיד והאינטרסים שלו. וגם אז, עליו לעשות כן רק מול גורמים מתאימים כגון יועץ/ת בית הספר.

7. **חובת אבטחת המידע –** בעל מאגר מידע, מחזיק במאגר מידע ומנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר (סעיף 17 לחוק) וכן לקיום ויישום תקנות אבטחת מידע.

חובות האבטחה על מאגר מידע

ריבוי המידע על אודות תלמידים המצטבר במאגרי מידע של מוסדות החינוך, במאגרים של בעלי המוסדות ושל גופים פרטיים הפועלים במערכת החינוך מחייב, כאמור, ניהול של המידע בצורה מושכלת והקפדה על אבטחת המידע הנאסף. תקנות אבטחת מידע מפרטות את אופן

יישומה של חובת אבטחת המידע המוטלת בחוק הישראלי על כל גורם המחזיק או מנהל מאגר מידע. התקנות חלות על כלל המשק הישראלי והן קובעות מנגנונים ארגוניים ודרישות מהותיות שמטרתן הפיכת אבטחת המידע לחלק משגרת הניהול השוטף של הארגון.

בפרק זה מובאים בתמצות העקרונות המרכזיים של אבטחת המידע במאגרי מידע בהתאם לחובות המפורטות בתקנות. בעלי ומנהלי מוסדות חינוך, גורמים שמוסדות אלו נמצאים בבעלותם או תחת אחריותם וגורמים פרטיים הפועלים במערכת החינוך (לרבות גורמים המחזיקים במידע על אודות תלמידים או ספקים במיקור חוץ) מחויבים להקפיד על יישום עקרונות אלה באופן שוטף, וכן בטרם הטמעת טכנולוגיות ומיזמים שונים.

מחובת כל גורם שבבעלותו מוסד חינוכי או גורם הפועל במערכת החינוך ואוסף או מחזיק במידע על אודות תלמידים להגדיר מהי רמת האבטחה החלה על כל אחד ממאגרי המידע שבבעלותו. בהתאם להגדרת רמת האבטחה החלה על המאגר, יבחן הגורם אילו הוראות בתקנות חלות על המאגר. כך למשל, **<u>רמת האבטחה הגבוהה</u> תחול על מאגר המכיל מידע אודות 100,000 אנשים ומעלה או שמספר בעלי ההרשאה לעיון ופעולות בו עולה על 100 מורשים ומטרתו העיקרית היא לדיווח ישיר, או שהוא כולל מידע הנוגע לצנעת חייו האישיים של אדם; מידע רפואי או מצב נפשי; מידע גנטי; עמדות פוליטיות או אמונות דתיות; עבר פלילי; נתוני תקשורת; נכסים והתחייבויות כלכליות והרגלי צריכה של אדם אשר יש בהם ללמד על מידע כאמור.** בכל הנוגע לתלמידים – מאגר מידע של משרד החינוך המכיל מידע הניתן לזיהוי על אודות כלל התלמידים עם צרכים מיוחדים בחינוך המיוחד, או על תלמידים הזכאים להקלות לימודיות בשל מצב בריאותי (ככל שמאגר שכזה אכן קיים), עשוי להיחשב כמאגר שחלה עליו רמת אבטחה גבוהה.

<u>יודגש, כי בכל הנוגע למוסדות חינוך רשמיים – בעל המאגר הוא משרד החינוך. בנוגע למוסדות חינוך שאינם רשמיים – בעל המאגר הוא הגוף שהמוסד החינוכי מצוי בבעלותו.</u> להלן מובאות בתמצות התקנות הרלוונטיות למאגרים:

1. **חובת בעל המאגר לנהל "מסמך הגדרות מאגר", לכל מאגר בכל רמת אבטחה** (תקנה 2). על בעל מאגר מידע לבחון את הצורך בעדכון המסמך אחת לשנה לפחות ובכל פעם שנעשה שינוי משמעותי, כמפורט בתקנה. המסמך יכלול: **תיאור כללי** של פעולות האיסוף והשימוש במידע, **תיאור מטרות איסוף המידע, תיאור סוגי המידע** השונים הכלולים במאגר, פרטים על העברת מאגר המידע או שימוש בו מחוץ לגבולות ישראל, האם נעשה **עיבוד באמצעות גורם זר או חיצוני** (לדוגמה: על אף שהמאגר מוחזק בשרתי המוסד החינוכי, המיזם ופלטפורמת עיבוד המידע מופעלות על ידי חברת "XYZ", המשמשת כספק חיצוני בהסכם), **מיפוי סיכונים** אפשריים ודרכי התמודדות עמם, **פרטים אישיים** של מנהל המאגר, מחזיק המאגר וממונה אבטחת המידע.

2. **חובת בעל המאגר למנות ממונה אבטחת מידע,** כנדרש בסעיף 17ב(א) לחוק, בהתאם לתנאים המפורטים בתקנה 3. תנאים ודגשים ספציפיים מובאים בהרחבה במדריך תקנות הגנת הפרטיות (אבטחת מידע) שפרסמה הרשות להגנת הפרטיות.[24]

3. **חובת בעל המאגר לקבוע, במסמך ברור, נוהלי אבטחת מידע, שמטרתם לייצר מדיניות אבטחת מידע עקבית בארגון,** כך שניתן יהיה להתמודד עם סיכוני אבטחה אליהם חשוף המידע (תקנה 4).

4. **בעל המאגר מחויב לבצע מיפוי של מערכות המאגר הנמצאות בבעלותו או בהחזקתו וכן סקר סיכונים.** כלומר, על בעל המאגר להכין מסמך מעודכן של מבנה מאגר המידע וכן רשימת מצאי מעודכנת של מערכות המאגר, הכוללת פרטים כמו: תשתיות ומערכות חומרה, סוגי רכיבים, תוכנות, ממשקים וכן פרטים נוספים המובאים בהרחבה בתקנה 5. **מאגר עליו חלה רמת האבטחה הגבוהה מחויב לערוך סקר סיכונים לאיתור סיכוני אבטחת מידע אחת ל-18 חודשים לפחות** ולפעול לתיקון ליקויים, אם התגלו. כמו כן, על מאגרים אלה חלה חובה לבצע **מבדקי חדירות** אחת ל-18 חודשים לפחות, לבחינת עמידותם.

5. **בעל מאגר מחויב להגן באופן פיזי על תשתיות החומרה המשמשות את המאגר,** במקום מוגן המונע כניסה ללא הרשאה. כמו כן, **בעל המאגר מחויב לתעד כניסת ויציאת עובדים מאתרים בהם מצויות המערכות** (מצלמות, זיהוי ביומטרי וכד'), כמפורט בתקנה 6.

6. **בעל מאגר מחויב למזער את הסכנה הפוטנציאלית שמציב הגורם האנושי** באמצעות העסקת עובדים אשר עברו הכשרות מתאימות בתחומי אבטחת המידע. בנוסף, **מחובת בעל המאגר לבחון את מידת התאמתם של עובדים אלה ולהעבירם הדרכות אחת לשנתיים,** לכל הפחות. בתוך כך, על בעל המאגר **לנהל הרשאות גישה למאגרים** בצורה מסודרת ואחראית, כמפורט בתקנות 7 ו-8.

7. **בעל מאגר מחויב לוודא שעובדים בעלי גישה למאגר הם אכן עובדים מורשים לכך, וזאת באמצעות זיהוי ואימות** (לכל הפחות באמצעות סיסמה). כמו כן, נדרש לנהל מנגנון המתעד באופן אוטומטי ועצמאי כל גישה למערכת, עליו תבוצע בקרה תקופתית, כמפורט בתקנות 9 ו-10.

24 | https://www.gov.il/BlobFolder/guide/data_security_guide/he/NEW_GUIDE.pdf.

8. **על בעל מאגר חלה החובה לתעד את כל אירועי האבטחה שהתרחשו, על מנת לייצר זיכרון ארגוני ביחס לאירועים חריגים ולהפיק מהם לקח לעתיד.** תקנה 11 מגדירה מהו "אירוע אבטחה חמור" כשמדובר במאגר עליו חלה רמת האבטחה הגבוהה, ומהו אותו אירוע כשמדובר ברמת אבטחה בינונית. במקרה של "אירוע אבטחה חמור" כהגדרתו בתקנות, **מחויב בעל המאגר להודיע על כך לרשות להגנת הפרטיות באופן מידי,** וכן לדווח על הצעדים שננקטו בעקבות האירוע. ניתן לדווח באופן מקוון באתר האינטרנט של הרשות להגנת הפרטיות.

9. **בעל מאגר מחויב להקפיד על מניעת זליגת מידע בעת שימוש בהתקנים ניידים** (מחשבים ניידים, טלפונים חכמים וכד'), במידת הצורך באמצעות הגבלת חיבור המאגרים להתקנים ניידים (תקנה 12). כמו כן, **יש להקפיד על ניהול מאובטח ומעודכן של מערכות המאגר** (תקנה 13). בנוסף, במידה שמערכות המידע והמאגרים מחוברים לרשת האינטרנט או לרשת ציבורית אחרת, **מחובת בעל המאגר לנקוט באמצעי אבטחה נוספים שימנעו גישה חיצונית ולא מורשית למידע** (תקנה 14).

10. **על בעל מאגר לנקוט משנה זהירות כאשר מוענקת גישה למאגרי המידע לגורמים חיצוניים בהתקשרות באמצעות מיקור חוץ** (כמפורט להלן גם בפרק ז' במדריך זה). עוד בטרם התקשרות במיקור חוץ על בעל המאגר, או מי הפועל מטעמו בהקשר זה, לבחון את סיכוני אבטחת המידע שבהתקשרות עם ספקים חיצוניים, ובמידה שהם גבוהים מדי להימנע ממיקור חוץ. כמו כן, יש לקבוע בהסכם מפורש עם הספק החיצוני קווים מנחים לפעילותו, בין היתר: סוג המידע אותו רשאי הספק החיצוני לעבד, המערכות אליהן רשאי לגשת, חובתו לסודיות ועוד (כמפורט בתקנה 15 וכן בהנחיית הרשות להגנת הפרטיות בנושא שימוש בשירותי מיקור חוץ לעיבוד מידע אישי).[25]

11. **בעל מאגר מחויב לערוך ביקורת פנימית או חיצונית, אחת ל-24 חודשים לפחות,** באמצעות גורם בעל הכשרה מתאימה, שאינו הממונה על אבטחת המאגר מטעמה, וזאת על מנת לוודא עמידה בתקנות, כמפורט בתקנה 16. ניתן לבצע את הביקורת במסגרת עריכת סקר סיכונים (כמוסבר בתקנה 5).

12. **בעל המאגר, או מי הפועל מטעמו בהקשר זה, מחויב להקפיד על משך זמן שמירת נתוני האבטחה ועל גיבוי ושחזור נתוני אבטחה,** שיש לבצע אחת לתקופה ובהתאם לדגשים המובאים בתקנות 18-17.

25 | הנחיית רשם מאגרי מידע מספר 2/2011 "שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי", https://www.gov.il/he/departments/policies/outsourcing

13. חשוב לזכור כי **חוק הגנת הפרטיות מטיל אחריות לאבטחת המידע במאגר על בעל המאגר, על מנהל המאגר ועל המחזיק המאגר.** גם הנחיות משרד החינוך הרלוונטיות, אשר יפורטו בהמשך, מטילות חלק מהחובות בהקשרים אלו **על מנהלי מוסדות החינוך המוגדרים על-ידי הנחיות אלו כמנהלי המאגרים.**

כמו כן, בסמכות הרשות להגנת הפרטיות לפטור מאגרים ספציפיים מחובות אבטחת מידע על פי התקנות, או לחלופין להטיל חובות נוספות בהתאם לנסיבות, כמפורט בתקנה 20.

מידע נוסף בנושא, ובכלל זה מדריך שאלות ותשובות בנושא תקנות אבטחת מידע, ניתן למצוא באתר הרשות להגנת הפרטיות.

פרק ז' | עקרונות להגנה על הפרטיות בעת הטמעת טכנולוגיות חדשות במוסדות החינוך

בפרק הקודם הוצגו העקרונות הבסיסיים המחייבים בחוק הגנת הפרטיות בנוגע לאיסוף ושימוש במידע אישי. עקרונות אלה מחייבים גם ביחס לטכנולוגיות מידע המצויות בשימוש מוסדות חינוך ומאגרי המידע הנוצרים במסגרת ותוך כדי פעילותם. **בפרק זה נפרט עקרונות נוספים אותם מומלץ למוסדות חינוך ובעליהם ליישם כדי להתמודד עם הסיכונים המוגברים לפרטיות – סיכונים הנובעים מן המאפיינים הייחודיים של שימוש מוסדות החינוך בטכנולוגיות מידע,** אשר תוארו והודגמו בפרקים הקודמים למדריך.

מומלץ שהבעלויות על מוסדות החינוך ומוסדות החינוך עצמם יפעלו בהתאם לעקרונות אלו בטרם מתקבלת החלטה על שימוש במיזם דיגיטלי חדש או על רכישה של טכנולוגיה או מערכת מידע חדשה. המלצתנו היא לקרוא עקרונות אלו כמבוא לנושאים שבמיקוד המפורטים בפרק הבא ובכאלו שהרשות להגנת הפרטיות תפרסם ותעדכן מעת לעת.

עיקרון האחריותיות וניהול מתכלל של שימוש בטכנולוגיות מידע במוסדות חינוך

אחד מיסודות הניהול הנכון של טכנולוגיות מידע טמון בהפנמה מוקדמת של שיקולי פרטיות באמצעות עיקרון "האחריותיות" (Accountability) וגישה מתכללת. עיקרון האחריותיות מתייחס לחובותיו של בעל מאגר מידע לפעול בהתאם לעקרונות עיבוד המידע הנדרשים על פי הדין ולהראות כי עמד בעקרונות אלו. עיקרון זה מחייב את בעלי מאגרי המידע ליישם אמצעים מתאימים ואפקטיביים שיבטיחו את יישום העקרונות הנדרשים ושיאפשרו גם את ההצגה של אופן היישום.

לאור האמור מומלץ שמוסדות חינוך ובעיקר הגורמים שמוסדות אלו נמצאים בבעלותם, ינקטו באמצעים ארגוניים, טכנולוגיים ומשפטיים שישפרו את מידת ה"אחריותיות" והמחויבות שלהם ליישום עקרונות הגנת המידע לצמצום הפגיעה של האמצעים הטכנולוגים השונים בפרטיות תלמידים.

תפיסה זו הפכה לפרקטיקה מקובלת בקרב גורמים המפעילים טכנולוגיות מידע בעולם, ובמקומות רבים, כגון באיחוד האירופי, תפיסה זו היא מחייבת גם מכוח דרישה חוקית

ורגולטורית מפורשת.[26] גם בישראל, ללא יישום עקרון האחריותיות, יתקשו מוסדות חינוך והגורמים שמוסדות אלו נמצאים בבעלותם לכבד את הזכות החוקתית של תלמידים לפרטיות, ויתקשה להימנע מפגיעה בפרטיותם במידה העולה על הנדרש.

יישום עיקרון זה בא לידי ביטוי, לדוגמה, במינוי גורם האמון על קביעת מדיניות כוללת בעניין שימוש בטכנולוגיות במוסדות חינוך, ואשר באחריותו לתכלל את הטיפול בטכנולוגיות אלו. בעידן של נתוני עתק (Big Data) וטכנולוגיות בינה מלאכותית, הסיכונים לפרטיות נובעים לא רק מהמאפיינים של כל פרויקט טכנולוגי בפני עצמו – אלא גם מהשפעות הגומלין בין הטכנולוגיות השונות ומהצלבת המידע הנאסף תוך כדי הפעלתן במקביל. לכן, נדרשת יד מכוונת ונקודת מבט מערכתית לשם הערכה מדויקת של הסיכונים לפרטיות והטיפול בהם.

במידה שקיים "ממונה על הגנת הפרטיות" (DPO), מומלץ שגורם זה יהיה אחראי על המשימה. "ממונה הגנת הפרטיות" הוא תפקיד שונה מ"ממונה אבטחת המידע", שעל פי הוראות חוק הגנת הפרטיות קיימת חובה למנות בגופים ציבוריים ובארגונים נוספים. תפקיד "ממונה הגנת הפרטיות" הוא בדרך כלל נושא משרה בכיר המרכז ועוסק בכל ההיבטים המשפטיים של הגנת המידע האישי במוסד החינוכי, ובמידת הצורך מנחה גם את ממונה אבטחת המידע. אם לא מונה עובד ייעודי הנושא בתפקיד ממונה על הגנת הפרטיות, ניתן להטיל את תכלול היבטי הפרטיות על ועדת היגוי ייעודית, צוות קבוע של ההנהלה הבכירה, וכדומה.[27]

יישום עיקרון האחריותיות והניהול המתכלל של שימוש בטכנולוגיות במוסדות חינוך נמצאים, ברמה העקרונית, תחת אחריות בעלי מוסדות החינוך. עם זאת, **כיום מספר הולך וגדל של מוסדות חינוך עוברים למודל של "ניהול עצמי", שמשמעותו העברת אחריות ניהולית לכתפיהם של מנהלי מוסדות החינוך תוך מתן אוטונומיה ועצמאות ניהולית ותקציבית למנהלים אלו.**[28] כחלק ממעבר למודל זה מתקשרים מוסדות החינוך באופן ישיר עם ספקי שירותים, לרבות של אמצעים טכנולוגיים. **בהינתן שהיבטים ניהוליים רבים עוברים לטיפול מנהלי מוסדות חינוך, מן הראוי כי כחלק מתהליך זה יפעלו המנהלים גם ליישום עקרון האחריותיות והניהול המתכלל של שימוש מוסדות החינוך בטכנולוגיות מידע.**

26 | עיקרון האחריותיות נקבע ברגולציית הגנת המידע של האיחוד האירופי GDPR - (General) Data Protection Regulation כעיקרון יסודי. להרחבה ראו רותם מדזיני "משטרי הגנת המידע באירופה: מעקרונות לתהליכים" **משפט, חברה ותרבות** ב37, 38 (2019).

27 | להרחבה ראו הרשות להגנת הפרטיות "מינוי ממונה הגנה על הפרטיות בארגון ותפקידיו" (29.10.20), https://www.gov.il/BlobFolder/rfp/refrences_dpo/he/DPO.pdf.

28 | יש הטוענים כי תהליך זה היו חלק מתהליך הביזור של מערכת החינוך, שבמסגרתו היבטים מסוימים עוברים מניהולו ואחריותו של משרד החינוך אל כתפי הנהלות בתי הספר. ראו למשל ניבי גל-אריאלי "אחריות מחולקת: על האחריות המשותפת של משרד החינוך ורשות החינוך המקומית לחינוך בישראל" 11 **דברים – כתב עת אקדמי רב תחומי** (נעימה ברזל עורכת, 2014).

דוגמה

בתקופת ההתמודדות עם נגיף הקורונה ולשם עמידה בצורך למדוד חום לתלמידים בכניסה למוסדות חינוך, החליטה רשות מקומית להפעיל במוסדות שתחת אחריותה מערכת טכנולוגיות למדידת חום המבוססת על זיהוי ביומטרי של תלמידים. המערכת מאפשרת למוסדות חינוך למדוד את חום התלמידים במקביל לרישום הנוכחות שלהם בכניסה, ולשם כך היא אוספת ומעבדת מידע ביומטרי של כלל התלמידים במוסדות החינוך בעיר.

יישום עקרון האחריותיות והגישה המתכללת צריכים להביא בהקשר זה את מנהלי מוסדות החינוך "להרים דגל", ולפנות לרשות המקומית ולגורמים רלוונטיים נוספים, כגון משרד החינוך, בדרישה לבחינה נוספת של המערכת. פנייה זו צריכה להיעשות לאור הפגיעה הפוטנציאלית בפרטיות תלמידים, שכן איסוף מידע ביומטרי על אודות תלמידים אינו מחויב לשם בדיקת מדדי חום בכניסה למוסדות חינוך, ולאור כך שניתן להשתמש באמצעים טכנולוגיים חלופיים ופוגעניים פחות להשגת מטרה זו.

תסקיר - בחינה מוקדמת של ההשפעה על הפרטיות

"תסקיר השפעה על פרטיות" (Privacy Impact Assessment) הוא הליך מובנה המנתח באופן מקיף ושיטתי את השפעת השימוש בטכנולוגיה על פרטיות נושאי המידע, מזהה את מכלול הסיכונים לפרטיות, בוחן חלופות ומציע את הדרך למזער אותם. לאור האמור מומלץ כי מוסדות חינוך ובעליהם יבצעו "תסקיר השפעה על פרטיות" בטרם יחליטו על שימוש במערכת טכנולוגיות בעלת פוטנציאל לפגיעה בפרטיות. הסיכונים הייחודיים והמוגברים לפרטיות תלמידים במוסדות חינוך מקנים משנה חשיבות להמלצה זו.

יצוין, כי עריכה מוקדמת של תסקיר חיונית לבחינת מידתיות השימוש בטכנולוגיות מידע, ומהווה אמצעי יעיל למימוש החובות שמטיל החוק על בעל מאגר. כמו כן, יצוין כי חלק מרכיבי התסקיר חופפים לדרישות הקיימות בסעיפים 2 ו–5 לתקנות אבטחת מידע המחייבות הכנת "מסמך הגדרות מאגר" ועריכת מיפוי של המערכות הטכנולוגיות המשמשות את המאגר.[29]

29 | לעיון במדריך הרשות להגנת הפרטיות בנושא תסקיר השפעה על פרטיות ראו:
https://www.gov.il/BlobFolder/generalpage/privacy_by_design/he/privacyimapctassessment2015.pdf

עיצוב לפרטיות

תפיסת העיצוב לפרטיות (Privacy By Design או PBD) ופרטיות כברירת מחדל (Privacy by Default) הן תפיסות הדוגלות בעיצוב מערכת המידע להגנה אופטימאלית על הפרטיות ולצמצום איסוף המידע ועיבודו למינימום ההכרחי, כבר משלב התכנון המוקדם ולאורך כל מחזור החיים של איסוף המידע והשימוש בו.

מומלץ כי מוסדות חינוך ובעליהם יפעלו בהתאם לעקרונות האמורים, וזאת למניעה מלכתחילה של כניסת טכנולוגיות למוסד החינוכי העלולות לפגוע בפרטיות תלמידים באופן שאינו מידתי. התנהלות בהתאם לעקרונות אלו צריכה להביא, בין היתר, ליישום מסקנות תסקיר השפעה על פרטיות.

שקיפות

שקיפות הוא אחד הכלים המרכזיים המאפשרים בקרה על אופן שימוש במידע על-ידי גורמים שונים, והכלי המרכזי המאפשר לנושא המידע לבחון ולבקר את אופן השימוש במידע הנוגע אליו.

לאור האמור על מוסדות חינוך ובעליהם מומלץ לנהוג בשקיפות ולהביא לידיעת ציבור התלמידים וההורים את הפרטים המהותיים הנוגעים לשימוש במידע אישי על אודותיהם: סוגי המידע הנאסף; השימושים שייעשו בו; האמצעים הננקטים לאבטחת המידע; סיכוני האבטחה; הגורמים אליהם המידע יהיה זמין ולאילו שימושים. כן יש להסביר לציבור התלמידים וההורים האם יש באפשרותם לבחור להימנע מאיסוף המידע על אודותיהם, כגון בדרך חלופית לקבלת שירות או שימוש בתשתית שלא כרוכה באיסוף מידע אישי. כמו כן, כחלק מהיבט השקיפות, הרשות ממליצה לפעול לשיתוף ולמעורבות תלמידים בתהליכי קבלת החלטות במוסדות חינוך, אשר עשויה להיות להן השפעה על פרטיותם.

יצוין כי סעיף 11 לחוק הגנת הפרטיות קובע כי בפניה לאדם לשם קבלת מידע על אודותיו (לשם איסופו או שימוש בו) יש לפרט בפניו האם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו, המטרה שלשמה מבוקש המידע, ולמי יימסר המידע ולשם איזו מטרה. את המידע האמור יש לפרסם במתכונת נגישה וברורה. רצוי שהמידע הרלבנטי יועבר לציבור התלמידים וההורים באופן ישיר על-ידי המוסד החינוכי וכן יהיה נגיש באופן מרוכז, למשל באזור ייעודי באתר האינטרנט של המוסד החינוכי או הרשות המקומית בה הוא פועל.

יצוין כי שקיפות צפויה גם להגביר את אמון ציבור התלמידים וההורים בטכנולוגיות בהן המוסד החינוכי משתמש.

דוגמה

מוסד חינוך החליט להתקין מצלמות מעקב בשטח המוסד. לשם כך, וליישום עיקרון השקיפות, החליט המוסד לשתף את התלמידים והוריהם בתהליך. במסגרת של פגישות עם נציגי הורים ותלמידים הציגה הנהלת המוסד את הסיבות לאורן יש לדעתה צורך בהצבת המצלמות, שמעה את דעתם בנושא ושיתפה פרטים שונים הנוגעים לאופן השימוש במצלמות, כגון מטרת השימוש במידע המצולם; זהות הגורמים שיהיו מורשים לצפות בחומרים; האמצעים הננקטים לשמירתו ואבטחתו של המידע המצולם; מיקום המצלמות וההגבלות השונות שיוטלו על אופן השימוש בהן. פירוט המידע, הכולל גם מידע בנוגע לזכויות של תלמידים והורים בנושא (כגון זכותם לעיין במידע), הועלה גם לאתר האינטרנט של המוסד ונשלח למייל של התלמידים והוריהם.

שימוש מוסדות חינוך במיקור חוץ ושיתוף פעולה עם גורמים מסחריים

תלמידים פוקדים את ספסל הלימודים מכוח הוראות חוק לימוד חובה המטיל חובה על הורים לשלוח את ילדיהם למוסדות חינוך מוכרים. במקרים רבים להורים ולתלמידים לא עומדת האפשרות לבחור את זהות המוסד החינוכי בו ילמד ילדם. כמו כן, במרבית המקרים, לתלמידים ולהוריהם לא עומדת האפשרות למנוע מהמוסד החינוכי להשתמש במערכות טכנולוגיות מידע שנועדו לצרכים חינוכיים, פדגוגיים או מערכתיים, או להגביל שימוש זה, חרף הפגיעה בפרטיות הכרוכה בכך.

משמעות הדבר היא שמידע רב על אודות תלמידים שבוי נאסף במסגרת מערכת החינוך, מבלי שלתלמידים או להוריהם עומדת האפשרות למנוע זאת או לשלוט על אופן השימוש בו. הנחת המוצא היא כי המידע האמור נאסף בהתאם להוראות הדין ומטעמים מוצדקים. עם זאת, בשל כך שמידע רב על אודות תלמידים נאסף למעשה ללא הסכמתם או הסכמת הוריהם, ובשל רגישותו של המידע, נדרשים מוסדות החינוך ובעליהם להקפדה יתרה בשיתופי פעולה עם גורמים מסחריים שבמסגרתם נאסף המידע.

לאור האמור, מכרזים או חוזים הנערכים בין מוסדות חינוך ובעליהם לבין גורמים מסחריים בנוגע לפרויקטים הכרוכים בהפעלת טכנולוגיית מידע במוסדות חינוך, ובאיסוף או בשימוש במידע על אודות תלמידים, חייבים לכלול בהתקשרות התייחסות מפורטת להיבטי פרטיות ואבטחת מידע, בהתאם להוראות תקנה 15 לתקנות אבטחת מידע ולהנחיית הרשות הגנת הפרטיות בנושא שימוש

בשירותי מיקור חוץ לעיבוד מידע אישי. כמו כן, בהתאם להנחיות משרד החינוך, מוסדות חינוך המבקשים להתקשר עם ספקים חיצוניים לרכישת או הפעלת אמצעים דיגיטליים שונים, מונחים שלא לעשות כן אלא באמצעות ספקים שאושרו על-ידי משרד החינוך.[30]

דוגמה

חברה טכנולוגית המפתחת סביבות תוכן טכנולוגיות למוסדות חינוך פיתחה סביבה אינטראקטיבית המאפשרת לתלמידים בגילאים שונים להתנסות בביצוע ניסויים מדעיים, וזאת מעבר לשעות הלימודים וכתמיכה לתכנים הנלמדים בשיעורי מדע. לשם שימוש בתוכנה נדרשים תלמידים לפתוח חשבון אישי בסביבת התוכן, והתוכנה מספקת למוסדות החינוך ניתוח על אודות התנהלות התלמידים במסגרתה, כגון נתונים בדבר הישגי התלמידים, מגמות השיפור שלהם, זמן פעילותם וכדומה.

המורה למדעים במוסד החינוך פנתה להנהלת המוסד בהצעה כי בית הספר יעשה שימוש בתוכנה. עם זאת, לאחר בדיקה, התברר להנהלת המוסד כי סביבת התוכן אינה מאושרת על-ידי משרד החינוך.

בפנייה למשרד החינוך נמסר להנהלת המוסד כי האישור לחברה הוסר כתוצאה מכשלים באבטחת מידע ואי-עמידה בהוראות תקנות הגנת הפרטיות (אבטחת מידע). כך, בין היתר, נמצא כי החברה העניקה הרשאות למידע לגורמים לא מאושרים, העבירה מידע לגורמים שלישיים (בניגוד להתחייבותה לא לעשות כן) ולא דיווחה למשרד החינוך על אירוע של אבטחת מידע שהתרחש מספר חודשים קודם לכן. לאור האמור הנחה משרד החינוך את הנהלת המוסד שלא להתקשר עם החברה.

30 | רשימת הספקים המורשים נמצאת באתר ה"קטלוג החינוכי". https://ecat.education.gov.il/.

פרק ח' | פרטיות תלמידים בעידן הדיגיטלי - נושאים במיקוד

ח.1 | החובות המוטלות על מנהל מוסד חינוכי בנושאי פרטיות במידע על אודות תלמידים

על מנהלים של מוסדות חינוך מוטלות חובות שונות בכל הנוגע להגנה על פרטיות תלמידים ומידע הנוגע אליהם. בראשית הדברים יש להבהיר כי בעוד הגורמים שמוסדות החינוך נמצאים בבעלותם הם אלו הנחשבים "בעלי המאגר", הרי שעל פי סע' 2.3 לחוזר מנכ"ל "מאגרי מידע בבתי ספר – רישום, דיווח ואבטחת מידע" תשע/3(א) מיום 1.11.09 (להלן: "חוזר מנכ"ל אבטחת מידע") מנהלי מוסדות חינוך הם מנהלי מאגרי המידע הפנימיים המצויים במוסד החינוכי.[31] בחלק זה יפורטו החובות המרכזיות המוטלות על מנהלי מוסדות חינוך בהקשר זה.

חובת רישום מאגר מידע

במוסדות חינוך רשמיים חובת רישום מאגר המידע מוטלת על משרד החינוך. לעומת זאת, על פי הנחיות משרד החינוך, במוסדות חינוך שאינם רשמיים, חובה זו מוטלת על מנהל המוסד.[32]

חובת דיווח למשרד החינוך

כל מנהל מוסד חינוך, רשמי או אחר, נדרש על פי הנחיות משרד החינוך לדווח למשרד החינוך על מאגרי המידע הנמצאים ברשות המוסד החינוכי. על פי הנחיות משרד החינוך, האחריות על דיווח למשרד על קיומם של מאגרי מידע (בכלל מוסדות החינוך, רשמיים ואחרים) היא של מנהל בית הספר, בין אם המידע מוחזק בבית הספר ובין אם הוא מוחזק אצל ספק או נותן שירות מטעם בית הספר.[33]

31 | https://cms.education.gov.il/EducationCMS/Applications/Mankal/EtsMedorim/3/3-6/HoraotKeva/K-2010-3a-3-6-8.htm.

32 | ראו סעיפים 4 ו- 5 לחוזר מנכ"ל אבטחת מידע.

33 | שם.

נחיצות מאגר המידע

על מוסדות החינוך להקפיד להחזיק אך ורק במאגרי מידע הדרושים להם לצורך עבודתם הסדירה וקיום תפקידיהם, ותו לאו. ככל שקיימים מאגרי מידע אשר אינם נדרשים לשם ביצוע עבודת המוסד החינוכי, יש לבחון את נחיצות שמירתו, וככל שאין כזו, רצוי להביא למחיקתו.

מטרת שימוש במידע

השימוש במידע ובנתונים השמורים במאגרי המידע מותר אך ורק לצורך המטרה שלשמה הוקם המאגר. שימוש שלא כדין במידע או שימוש במאגרי מידע שלא נרשמו כדין אסור על פי החוק, ועלול אף להיחשב עבירה פלילית.

יישום כללי אבטחת מידע

על פי הנחיות משרד החינוך ובין היתר כמפורט בסעיף 6 לחוזר מנכ"ל אבטחת מידע, מנהל המוסד החינוכי הוא האחראי על יישום כללי אבטחת המידע במוסד החינוכי. לאור האמור, על המנהל מוטלת האחריות לדאוג, בין היתר, להיבטים הבאים:[34]

- אבטחה פיזית של המחשבים ושל המידע השמור בהם.
- אבטחה לוגית של הגישה למידע ושל השימוש המותר בו באמצעות סיסמאות גישה חסויות שתימסרנה רק למורשי גישה למאגר המידע.
- פיקוח על עובדים הבאים במגע עם מידע רגיש או מוצבים בתפקידים רגישים העושים שימוש במאגרי מידע, וכן על עובדים (לרבות קבלנים, ספקים ועובדיהם) העושים שימוש במערך השליטה והבקרה הטכנולוגיים על מאגרי המידע.
- הכנת גיבויים ושמירתם במקום מאובטח.
- היה ובית הספר מאפשר לסגל החינוכי או לתלמידים להוציא מחשבים מחוץ לכותלי בית הספר, יש לוודא כי על המחשבים מותקנת תוכנת אנטי וירוס מעודכנת; כי מערכת ההפעלה מתעדכנת באופן שוטף וכי לא נשמר או מגובה על המחשבים מידע אישי ורגיש.
- על כלל מערכות המחשב בבית הספר להימצא מאחורי "חומת אש" היקפית אשר מנוהלת ומתוחזקת באופן שוטף. יש להגדיר ב"חומת האש" הפרדה בין הרשת המנהלתית בבית

34 | יודגש כי הפירוט להלן אינו ממצה וכי קיימות חובות נוספות המוטלות על מנהל המוסד. לפירוט מלא ראו הנחיות משרד החינוך המפורטות בסוף הפרק.

הספר הכוללת את מחשבי המזכירות, מנהל בית הספר וכדומה לבין הרשת הפדגוגית הכוללת את מחשבי המעבדה, כיתות המחשבים וכדומה.

- בבית ספר שבו קיימת רשת אלחוטית Wi-Fi יש להגדיר את הגישה אליה בסיסמה. את הסיסמא יש לשנות אחת לשנה.
- לצרכים פדגוגיים ומנהלתיים על מנהל המוסד לוודא כי בית הספר משתמש אך ורק בדוא"ל ארגוני מאובטח ולא בחשבונות דוא"ל פרטיים.
- יש להקפיד כי במקומות בהם נעשה שימוש לשמירת מידע מוגן על פי חוק הגנת הפרטיות (לסוגי המידע שהחוק מגן עליהם ראו גילוי דעת הרשות להגנת הפרטיות בנושא 'מהם "מידע" ו"ידיעה על ענייניו הפרטיים של אדם" בחוק הגנת הפרטיות'), הגישה למידע תבוצע באמצעות הרשאות גישה שונות לאנשי הצוות. הרשאות הגישה ינוהלו כך שרק לבעלי התפקידים הרלבנטיים תהיה גישה למידע הרלוונטי להם. כך למשל יש להקצות ליועצת בית הספר ספריית רשת נפרדת אשר רק לה תהיה גישה לתכניה.

מינוי ממונה אבטחת מידע

בהתאם לסעיף 2.4 לחוזר מנכ"ל אבטחת מידע מנהל מוסד חינוך רשאי למנות ממונה אבטחת מידע, אשר יהיה ממונה על הניהול השוטף של מערך אבטחת המידע במוסד החינוכי. אם לא מונה אדם אחר לתפקיד זה – מנהל המוסד משמש גם כממונה אבטחת המידע. ממונה אבטחת המידע יהיה אחראי, בין היתר, על מתן הרשאות שימוש במידע ובמאגרי מידע ויפקח על קיום נוהלי השמירה ואבטחת המידע, לרבות דיווח על אירועי אבטחת מידע (גניבה, כניסה לא מורשית למאגרי המידע או למערכות המחשוב בבית הספר). ממונה אבטחת המידע פועל תחת פיקוחו של מנהל המוסד החינוכי.

שימוש ספקי תוכנות השלמה במידע

על מנהל המוסד החינוכי/הממונה על אבטחת המידע לבקש מהספקים של תוכנות השלמה העושות שימוש במאגר המידע של המנב"ס (מערכת ניהול בתי ספר) להעביר אישור מגורם בלתי-תלוי ומוכר בתחום אבטחת המידע על התקינות של אבטחת המידע בתוכנה. ללא אישור זה אין להתקין את התוכנה בבית הספר, אין לאפשר לספק התוכנה גישה למאגרי המידע וכן אין להעביר אליו מידע ונתונים על תלמידים ומורים בכל דרך שהיא.

עם סיום ההתקשרות בין בית הספר לבין הספק, יש לוודא כי כל הנתונים הוחזרו לבית הספר באופן שניתן להמשיך ולהשתמש בהם וכן כי הספק ביער לחלוטין את הנתונים במאגרים שלו, ואין בחזקתו נתונים של בית הספר בכל מדיה שהיא.

האחריות על מאגרי המידע אשר הועברו על ידי בית הספר לספקים חיצוניים/ליישומים חיצוניים/לתוכנות השלמה וכדומה, לרבות בכל הנוגע ליישום חובות אבטחת המידע המצוי במאגרים אלה, חלה על מנהל המוסד החינוכי.

שמירת מידע מוגן

באחריות מנהל המוסד החינוכי לוודא כי מידע מוגן על אודות תלמידים על פי חוק הגנת הפרטיות (ובכלל זה נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו),[35] יישמר אך ורק במקומות המתאימים לכך. לפי הנחיות משרד החינוך, מידע מוגן שכזה ניתן לשמור במקומות הבאים:[36]

- מערכות משרד החינוך;
- מוצרים חינוכיים טכנולוגיים מאושרים על ידי משרד החינוך מטעם ספקים מורשים (רשימת הספקים המורשים מפורסמת באתר ה"קטלוג החינוכי");
- ספריות רשת ייעודיות בשרת בית הספר;
- סביבות ענן בית ספריות מסוג Microsoft Office 365 for Education.

אין "להוריד" ולשמור מידע מוגן על פי חוק הגנת הפרטיות במחשבים פרטיים של עובדי המוסד החינוכי; בהתקנים ניידים (דיסק און קיי); במחשבי בית ספר שברשת הפדגוגית; במחשבים "ציבוריים" שבבית הספר; בחשבונות ענן פרטיים, והכל אף לא לפרק זמן מוגדר.

35 | לפירוט עמדת הרשות להגנת הפרטיות בנושא הגדרת "מידע" על-פי חוק הגנת הפרטיות, ראו מסמך "גילוי דעת: מהם 'מידע' ו'ידיעה על ענייניו הפרטיים של אדם' בחוק הגנת הפרטיות", לעיל ה"ש 3.

36 | ראו מסמך "מדיניות שמירה וטיפול במידע מוגן במוסדות חינוך", לעיל ה"ש 4.

שמירת פרטיות ואבטחת מידע ביישומי ענן

מנהל מוסד החינוך הוא האחראי לקיום הנחיות אבטחת המידע בבתי הספר בסביבות יישומי ענן. לשם כך, על מנהל המוסד לפעול, בין היתר, על פי הכללים הבאים:

- בעת פתיחת הסביבה יש להגדיר מנהלים לסביבה (אדמיניסטרטורים) מטעם בית הספר. מנהלי הסביבה יכולים להיות מנהלי המוסד החינוכי, רכזי התקשוב, מתאמי המחשוב או גורם אחר מסגל בית הספר שאותו ממנים המנהלים.
- על כלל מנהלי סביבות הענן לעשות שימוש בהזדהות חזקה הכוללת סיסמה אישית חזקה ומנגנון לאימות דו-שלבי (Two Factor Authentication).
- רק תלמידים ואנשי הצוות החינוכי של המוסד רשאים לעשות שימוש בסביבות הענן. אין לצרף לסביבה גורמים חיצוניים מחוץ לאוכלוסיית החינוך של בית הספר.
- אין לייצר ממשקים בין סביבות הענן למערכות מידע ואפליקציות חיצוניות.

מקורות

חוזר מנכ"ל מאגרי מידע בבתי הספר – רישום, דיווח ואבטחת מידע
https://cms.education.gov.il/EducationCMS/Applications MankalEtsMedorim/3/3-6/ /HoraotKeva

הנחיות אבטחת מידע למוסדות חינוך
https://sites.education.gov.il/cloud/home/tikshuv/Documents/hanchayot_havtachat_mida_batisefer.pdf

מדיניות שמירה וטיפול במידע מוגן במוסדות חינוך
https://sites.education.gov.il/cloud/home/havtachat_mida/Documents/mediniyut_shmira_vetipul_bemeyda_mugan_bemosadot.pdf

הנחיות והמלצות לסביבות ענן לחינוך
https://sites.education.gov.il/cloud/home/svivot_anan_hinuch/Pages/havtacha.aspx

ח.2| טכנולוגיות מעקב בשטח המוסד החינוכי

כפי שצוין קודם לכן, מוסדות חינוך רבים בארץ ובעולם עושים שימוש בטכנולוגיות למעקב אחר מיקום והתנהלות תלמידים.[37] כאמור, שימוש מוסדות חינוך בטכנולוגיות מעקב טומן בחובו פוטנציאל לפגיעה בפרטיותם של תלמידים.

בחלק זה נפרט על הכללים המרכזיים החלים ביחס לשימוש מוסדות חינוך לילדים מגילאי שלוש ומעלה במצלמות מעקב המהוות, נכון למועד כתיבת שורות אלו, טכנולוגיית המעקב המרכזית בה משתמשים מוסדות חינוך בישראל. פירוט זה ייעשה בעיקרו לאור הוראות חוזר מנכ"ל "מצלמות במוסדות החינוך – הסדרת הכנסתן ואופן התקנתן" (הוראת קבע מס' 119), מיום 3.5.2015 (להלן: "חוזר מנכ"ל מצלמות מעקב").[38] בהמשך נתייחס לאופן ההתנהלות המומלץ למוסדות חינוך אלו ביחס לשימוש בטכנולוגיות מעקב נוספות. יובהר כי מסמך זה לא מתייחס לסוגיית ההתקנה והשימוש במצלמות במעונות יום לפעוטות מגילאי לידה עד שלוש.[39]

ח.2.א | טכנולוגיות מעקב בשטח המוסד החינוכי

להלן יפורטו הכללים המרכזיים ביחס לשימוש במצלמות למעקב אחר התנהלות תלמידים בשטח המוסד החינוכי. יצוין כי בהתאם להנחיות משרד החינוך ניתן לזהות שלושה סוגים של מצלמות המובחנות ביחס לתכלית השימוש בהן:

- מצלמות למעקב אחר התנהלות תלמידים בשטח המוסד החינוכי ובשעות הלימודים (להלן: "מצלמות מעקב");
- מצלמות לשמירה על רכוש המוסד החינוכי, המופעלות בשעות שלאחר פעילות תלמידים במוסד החינוכי (להלן: "מצלמות להגנה על רכוש");
- מצלמות אבטחה המיועדות לשמירה על ביטחון התלמידים מפני גורמים חיצוניים למוסד החינוכי, ואשר מופנות לשטחים שמחוצה לו (להלן: "מצלמות אבטחה").

37 | נכון לעת כתיבת המדריך, ולמיטב ידיעת משרד החינוך, מוסדות חינוך בישראל עושים בעיקר שימוש במצלמות ולא בטכנולוגית מעקב אחרות. הנחת המוצא היא כי שימוש מוסדות חינוך במצלמות מעקב נעשה בהתאם להוראות חוזר מנכ"ל משרד החינוך המסדיר את אופן השימוש במצלמות, ושעקרונותיו יפורטו בהמשך.

38 | https://apps.education.gov.il/mankal/horaa.aspx?siduri=134#_Toc256000072.

39 | לאופן הסדרת השימוש במצלמות במעונות יום לפעוטות, ראו: חוק התקנת מצלמות לשם הגנה על פעוטות במעונות יום לפעוטות, התשע"ט-2018. להרחבה ראו: הרשות להגנת הפרטיות "כללים ליישום חוק התקנת מצלמות לשם הגנה על פעוטות במעונות יום לפעוטות, התשע"ט-2018", (19.10.20) https://www.gov.il/BlobFolder/news/cameras_daycare_guide/he/camera.pdf.

עיקר הכללים שיפורטו להלן עוסקים במצלמות מעקב מהסוג הראשון. בסיפא הדברים נתייחס למצלמות אבטחה מהסוג השלישי:

מידתיות השימוש במצלמות מעקב

בכל מקרה של כוונה להציב מצלמות מעקב בשטח המוסד החינוכי יש לבדוק אם מצלמות המעקב הן האמצעי המתאים והיעיל להשגת המטרה הרצויה, ולברר אם אפשר להשיג מטרה זו באמצעי הפוגע פחות בפרטיות. ככל שאפשר להשיג את המטרה באמצעי פוגעני פחות – יש לעשות שימוש באמצעי זה ולהימנע משימוש במצלמות.

יש לשקול בכובד ראש את עצם השימוש במצלמות מעקב, ואם הוחלט לעשות בהן שימוש, יש לעשות כן במידה שאינה עולה על הנדרש לשם השגת המטרה שבעטיה הוצבו המצלמות מלכתחילה. כך למשל, **מספר המצלמות שיותקנו צריך להיות המספר המינימלי החיוני** להשגת המטרה.

מיקום מצלמות וזווית הצילום

ניתן להתקין מצלמות מעקב אך ורק בשטחים הציבוריים של המוסד החינוכי (חצר, מסדרונות). חל איסור על הצבת מצלמות במתחם הפנימי של מוסד החינוך, קרי בכיתות, בחדר היועצ/ת וכדומה. כמו כן, **חל איסור** על הצבת מצלמות במתחם הפנימי של גני ילדים לילדים מגילאי שלוש ומעלה.

זוויות הצילום וגזרת הצילום יוגבלו באופן שיכסו רק את השטחים הרלוונטיים ויקלטו באופן המזערי האפשרי את השטח שאינו רלוונטי למטרת הצבתה של המצלמה.

במקרה של מצלמות מעקב שיוחלט להציבן בסמוך למקום שמתקיימת בו פעילות פרטית או מעין פרטית ברשות היחיד, כגון חדרי השירותים, חדרי הכיתות, המרפאה וחדר היועצ/ת, תוצב המצלמה באופן המגביל את יכולת הצפייה והצילום של שטחים אלה **והמקום לא יצולם**.

יכולות מצלמות המעקב

ככלל יהיה הצילום בגודל אחיד, ללא יכולת לשינוי רזולוציית צילום. **חל איסור לחבר למצלמות התקנים בעלי יכולת הקלטת שמע** ("אודיו").

תכלית צפייה בחומרים המצולמים במצלמות מעקב

צפייה בחומרים המצולמים במצלמות המעקב, אם בזמן אמת ואם לאחר מכן, תהא אך ורק לתכלית של איתור או בדיקת אירועי אלימות ובריונות, התנהגויות סיכון כגון עישון ושתיית אלכוהול, וסיכוני בטיחות הנובעים מהתנהלות של גורם אנושי. **פרט למטרות אלו אין לעשות שימוש במצלמות או בחומרים המצולמים על-ידן.**

כך לדוגמה, שימוש במצלמות ובחומרים המצולמים לאיתור העתקות בבחינות או לבדיקת נוכחות תלמידים בבית הספר היא **אסורה**.

כפי שצוין קודם לכן, מוסדות חינוך רשאים להשתמש במצלמות גם לתכלית של שמירה על רכוש בית הספר או גן הילדים (כגון מחשבים, ציוד מעבדות וכדומה). עם זאת, במצלמות אלו לא ייעשה שימוש ואין לאפשר את פעילותן כל זמן שמתקיימת במבנה המוסד החינוכי פעילות של ילדים.

כללים בדבר צפייה בחומרים המצולמים ממצלמות מעקב

אפשרות הצפייה במצלמות מעקב ובחומר המצולם תהיה רק בחדר המנהל.

בצילום בזמן אמת יהיה רשאי לצפות מנהל בית הספר, או מי שהוסמך על ידו לכך מהצוות של בית הספר. צופה לא יהיה רשאי לעשות שימוש במידע הנובע מהצפייה או לגלותו למי שלא הוסמך לכך, אלא לצורך מילוי תפקידו.

בחומר המוקלט יהיו רשאים לצפות מנהל בית הספר, סגנו, היועץ החינוכי ופסיכולוג בית הספר. אם המנהל החליט כי על איש צוות חינוכי לצפות בחומר מוקלט מסוים, תתאפשר הצפייה באותו חומר מוקלט רק בנוכחות המנהל במהלך הצפייה. עצם ההחלטה על הצפייה בחומר המוקלט ועל תדירותה, במקרה שלא נתקבל מידע על אירוע מסוגי האירועים שצוינו קודם לכן (אירועי אלימות וכדומה) נתונה לשיקול דעת המנהל, אך גם זאת תהא אך ורק במטרה לאתר אירועים שכאלו.

שמירת החומר המוקלט ממצלמות מעקב

את החומר שיוקלט יש למחוק לאחר 3 ימים מיום שהוקלט לכל המאוחר, אלא אם כן סבר מנהל המוסד החינוכי שההקלטה כוללת אירוע אלימות או בריונות חריג, או אם מדובר בסיכוני בטיחות חריגים הנובעים מהתנהלות של גורם אנושי המצריכים התייחסות, וזאת בכפוף לקבלת האישורים הנדרשים, כמפורט בסעיף 2.4.3 לחוזר מנכ"ל מצלמות מעקב.

האירוע המסוים יועתק ויישמר בנפרד משאר החומרים בכספת שבחדר המנהל. אין לשמור קבצים מועתקים על מחשבים. לאחר 7 ימים יש לערוך בחינה חוזרת של הצורך בשמירת החומר המוקלט. עם תום הטיפול באירוע – יימחק ויבוער החומר המצולם, וכל העתק שלו.

במקרה שמדובר באירוע חריג שהוא נזיקי או תאונה או שיש בו מפגע מיוחד, ישמור המנהל העתק של צילום האירוע, וכן יעביר העתק שלו לקב"ט המחוז של משרד החינוך. העתק יישמר בכספת בית הספר, שתהיה מאובטחת, והגישה אליה תהיה נתונה רק למנהל בית הספר או למורשה מטעמו.

עיון בחומר המוקלט

לאדם המצולם והמתועד בחומר הצילום ממצלמות המעקב, לרבות ילדים, יש זכות לעיין בחומר. עם זאת, מנהל המוסד לא יאפשר עיון במידע אלא בתנאים הבאים:

- הבקשה לעיון הוגשה על-ידי גורם בעל עניין והיא קיבלה אישור של המפקח הכולל של המוסד החינוכי לאחר היוועצות עם היועץ המשפטי הרלוונטי (במוסד חינוך בבעלות פרטית – ביועץ המשפטי של הבעלים על בית הספר; במוסד חינוך רשמי – ביועץ המשפטי של משרד החינוך).
- דמותם ותווי הפנים של אנשים נוספים הנמצאים בצילום יטושטשו כך שלא יהיה ניתן לזהותם. אם טשטוש זהותם של אנשים נוספים בצילום דורש הקצאת משאבים בלתי סבירה, או אינו אפשרי מסיבה אחרת, לא יימסר למבקש העתק של החומר המוקלט.
- הצופה במידע לא ייחשף לחומר המוקלט מעבר לזה שהוא זכאי לעיין בו.
- הצפייה תיערך בחדר המנהל ובנוכחותו.

אין באמור לעיל כדי למנוע עיון ומסירת העתק של חומר מוקלט המחויבת בהתאם להוראות כל דין, ובכלל זה מסירת מידע לרשויות הביטחון לפי דרישה חוקית או מסירת מידע לבית משפט מוסמך לפי החלטה שניתנה על ידו.

שיתוף ויידוע ציבור בנוגע לשימוש במצלמות מעקב

יש לשתף את קהילת בית הספר (המורים, התלמידים וההורים) בנושא ולרתום אותם למען המטרות שלשמן הוצבו מצלמות המעקב. אם הוחלט על הצבת מצלמות בתחום המוסד החינוכי, יש למסור על כך הודעה לציבור ההורים והתלמידים אשר תפרט את

האזורים שבהם יופעלו המצלמות. כמו כן, על המוסד החינוכי לתלות מודעות בעניין בכניסה לשטח המוסד וכן בקרבת מיקום הצבתה של כל מצלמה. מעבר לכך, יש לקיים לפחות פעילות אחת בנושא במהלך שנת הלימודים עם המורים ועם התלמידים.

הוראות אלו לא חלות לגבי מצלמות אבטחה המותקנות לצרכי ביטחון, ואין חובה לפרסם את המקומות בהן מותקנות מצלמות שכאלו ומצלמות שנועדו לצורך שמירה על רכוש.

בקרה

על מנהל המוסד החינוכי, או מנהל מחלקת החינוך ברשות החינוך המקומית (לפי העניין), להעביר מדי שנה דיווח עתי, במסגרת הדיווחים המוגשים למשרד החינוך, שיכלול את הפרטים הבאים: נתונים בדבר מצלמות שהותקנו במוסד החינוך בשנה החולפת ופרטים בדבר מצלמות שהוסרו.

אבטחת מידע

בנוסף לכללי אבטחת המידע שפורטו קודם לכן, מוסד חינוכי המשתמש במצלמות מעקב מחויב לפעול, בין היתר, גם לפי הכללים הבאים:

- המצלמות יחוברו ברשת מבודדת מרשתות אחרות ומרשת האינטרנט. המידע עצמו יאובטח לוגית על השרת באמצעות מערכת ניהול הרשאות;
- גישה פיזית למצלמות ולתשתית תינתן למורשים בלבד ורק במידת הצורך, כגון תיקון, שדרוג וכדומה;
- הכניסה לאזור השרת המנהל את המצלמות תהיה מבוקרת, ובכלל זה ליווי הגורם הנכנס ותיעוד הכניסה ביומן רישום אירועים;
- השרתים והציוד המשמשים לאחסון, לעיבוד ולגישה לשרת המנהל את המצלמות ואת מערכת ההקלטה והיישומים, יהיו מוגנים על ידי אמצעים מתאימים לבקרת כניסה כדי להבטיח שהגישה תותר רק לעובדים מורשים;
- גישה לחומר המוקלט תותר לרשימת מורשים לפי הקבוע בהנחיות סעיף 7.3 לחוזר מנכ"ל מצלמות מעקב;
- ייושמו אמצעי אבטחה הולמים שימנעו חדירה מכוונת או מקרית למערכת או למערכות התשתית והתקשורת של המצלמות;

- המערכות השונות למניעת ניצול פרצות אבטחת מידע יעודכנו באופן שוטף;
- מנהל מוסד החינוך ידווח באופן מיידי לקב"ט מוסדות החינוך ברשות המקומית בכל מקרה של חשש לדליפת מידע או לשימוש חורג מההרשאה שניתנה.

עד כאן הכללים המרכזיים ביחס לשימוש במצלמות למעקב אחר התנהלות תלמידים בשטח הפנימי של המוסד החינוכי. להלן נתייחס בקצרה גם למצלמות אבטחה המותקנות לפיקוח על האזורים שמחוץ לשטח המוסד.

שימוש במצלמות אבטחה

מוסדות חינוך רשאים להשתמש במצלמות גם לצורכי אבטחה. מצלמות אלו יוצבו **על הגדר ההיקפית של המוסד החינוכי, ופני המצלמה יופנו כלפי חוץ,** ללא כוונה לצלם תלמידים (אלא באופן אגבי, לכל היותר).

מצלמת אבטחה תוצב באופן שתצלם את השטח הציבורי בלבד. בבתי הספר ימוקמו מצלמות האבטחה ברחבה המובילה לבית הספר, ויצפו על שערי הכניסה לבית הספר ועל הגדרות המקיפות את בית הספר כלפי השטחים שמחוץ לבית הספר. בגני ילדים לילדים מגילאי שלוש ומעלה יתמקדו מצלמות האבטחה רק בתצפית על שער הגן, על שביל הגישה לגן ובגדרות המקיפות את הגן כלפי השטחים שמחוצה לו.

ההחלטה על הצבת מצלמות אבטחה בתחום ההיקפי של בית הספר לצורך הפעלתן **בשעות הלימודים** תהיה של הבעלים על מבנה המוסד החינוכי או של רשות החינוך המקומית או של גורמי הביטחון, **בהתייעצות עם מנהל המוסד החינוכי** ובתיאום עם קב"ט הרשות המקומית או עם קב"ט מחוז משרד החינוך ועם משטרת ישראל.

ח.2.ב | שימוש בטכנולוגיות חדשות למעקב במוסדות החינוך

כאמור, מצלמות במעגל סגור הן טכנולוגיות המעקב השכיחות ביותר הנמצאות כיום בשימוש מוסדות החינוך בישראל. השימוש בטכנולוגיות אלו מוסדר תחת הנחיות משרד החינוך שעיקרן פורט לעיל.

עם זאת, מוסדות חינוך במדינות שונות בעולם עושים שימוש בטכנולוגיות מעקב מסוגים שונים, כגון מערכות ביומטריות בכניסה למוסדות חינוך, מערכות מבוססות טכנולוגיית RFID למעקב אחר מיקום תלמידים בשטח המוסד החינוכי ומערכות מבוססות אינטליגנציה

מלאכותית (AI) לניטור התנהלותם של תלמידים במהלך השיעורים.[40]

גם בישראל ניתן לזהות ניצנים של ניסיונות לשימוש במערכות טכנולוגיות חדשות למעקב אחר תלמידים. כך, לפי פרסומים בתקשורת, במוסדות חינוך נעשה בעבר ניסיון להשתמש במערכות ביומטריות במסגרת כניסת תלמידים למוסדות חינוך.[41] כמו כן, בתקופת ההתמודדות עם נגיף הקורונה פורסם על אפשרות של שימוש מוסדות חינוך בטכנולוגיות שונות, כגון טכנולוגיה תרמית למדידת חום מרחוק, אשר יסייעו למוסדות חינוך בבדיקת חום גופם ומצבם הרפואי של תלמידים.[42]

שימוש במערכות טכנולוגיות האוספות מידע אישי מזוהה או ניתן לזיהוי ומשתמשות במידע אישי לצרכי מעקב אחר תלמידים, כגון מערכות ביומטריות או מערכות לזיהוי פנים, עלול לפגוע קשות בפרטיות תלמידים, כפי שפורט בפרק ה' למדריך זה.

לאור האמור, עמדת הרשות להגנת הפרטיות היא כי על מוסדות חינוך להימנע משימוש במערכות שכאלו. שימוש בטכנולוגיות כאלו צריך להיעשות, אם בכלל, רק לאחר קבלת אישור מטעם הגורמים הרלוונטיים במשרד החינוך ורק לאחר שגורמים אלו בחנו את הצורך בשימוש במערכות, את החלופות האפשריות להן וערכו תסקיר השפעה על פרטיות ביחס להשפעתן על פרטיותם של תלמידים.

לפיכך, הרשות להגנת הפרטיות ממליצה כי מוסדות חינוך או גורמים שמוסדות אלו נמצאים בבעלותם, השוקלים שימוש בטכנולוגיות חדשות למעקב אחר התנהלות תלמידים במרחב הבית-ספרי, יפנו בעניין זה לגורמים הרלוונטיים במשרד החינוך, **בטרם יעשו כל שימוש בטכנולוגיות האמורות.**

40 | מערכות מבוססות אינטליגנציה מלאכותית לניטור התנהלות תלמידים נמצאות כיום בשימוש בעיקר במוסדות חינוך בסין. מערכות אלו מנטרות את תווי הפנים של תלמידים בעודם לומדים בכיתה, ומנתחות, בין היתר, את מידת הריכוז והקשב של התלמידים ואת רגשותיהם במהלך השיעור.

41 | אביגיל קדם "הורים: שערים ביומטריים? לא בבית ספרנו" **mynet** (11.12.14), https://rishon.mynet.co.il/local_news/article/m_129155. בכתבה מצוין כי ניסיון להתקנת שער ביומטרי במוסד חינוכי נעשה כבר בשנת 2009.

42 | שגיא כהן "גם בגנים ובבתי ספר? בקרוב מצלמות אבטחה חכמות ימדדו לכם חום בכל מקום" **TheMarker** (21.4.20), https://www.themarker.com/coronavirus/.premium-1.8787285.

ח.3 | שמירת מידע על האודות תלמידים במערכות לניהול פדגוגי

מוסדות חינוך רבים משתמשים במערכות לניהול פדגוגי מבוסס נתונים. מערכות אלו מאפשרות, בין היתר, שמירה ותיעוד של מידע על אודות תלמידים, את העברתו של המידע בין גורמים שונים במוסד החינוכי ומחוצה לו,[43] וכן את עיבודו של המידע לצרכים שונים. מערכות אלו נחשבות ככאלו העשויות להקל משמעותית על זרימת המידע והתקשורת במעגלים השונים של הארגון החינוכי.

התפיסה החינוכית המקובלת היא כי הטמעת מערכות מתוקשבות לניהול פדגוגי עשויה לקדם תחומים הקשורים לאפקטיביות הבית ספרית וזאת, בין היתר, הודות לאפשרות המעקב אחר תפקוד המורים והתלמידים וחיזוק התקשורת בתוך צוות המורים ובינם לבין הורים ותלמידים. ככלל, שימוש מוסדות חינוך במערכות אלו נעשה בהתאם למדיניות משרד החינוך.

חרף היתרונות שבשימוש במערכות מתוקשבות לניהול פדגוגי מבוסס נתונים, שימוש זה – ובמיוחד מכיוון שמרבית מערכות אלו מאפשרות להורים ולתלמידים גישה למידע "מרחוק" – עלול לפגוע בפרטיותם של תלמידים, וזאת בשני היבטים מרכזיים:

חשיפת מידע רגיש על אודות תלמידים

כידוע, מערכות טכנולוגיות אינן חסינות מפני מצבים של חדירה וזליגת מידע. מצב זה נכון גם ביחס למערכות לניהול פדגוגי. כאמור, במערכות אלו נשמר מידע רב על אודות תלמידים, שחלקו אף עשוי להיחשב מידע רגיש. במצב זה קיים חשש כי מידע זה עלול לזלוג ולהיחשף ברבים.

דבר זה נכון ביתר שאת ביחס למערכות לניהול פדגוגי המאפשרות למשתמשים (הורים ותלמידים) גישה "מרחוק" למידע השמור בהן. בעניין זה יש לזכור כי רבים מההורים והתלמידים ניגשים למידע שבמערכות אלו מתוך מערכות שאינן מאובטחות דיין וכן מהטלפון החכם שלהם (ושחלקם אף אינם מבצעים התנתקות מלאה ביציאה מהמערכות). כל האמור מחדד את **החשש כי המידע השמור במערכות האמורות יזלוג וייחשף בפני גורמים לא מורשים, ולפגוע גם בכך פרטיותם של תלמידים.**

יצוין כי הנחיות משרד החינוך אינן מבהירות איזה מידע יש להעלות ולשמור במערכות לניהול פדגוגי, איזה חלקים מתוך מידע זה ניתן להנגיש להורים ולתלמידים באמצעות הרשאות לגישה מרחוק, ואיזה מידע רצוי להימנע לשמור ולהעלות במסגרתן. לאור האמור

43 | בעיקר להורים ולגורמים שונים במערכת החינוך, והכל במסגרת מדיניות משרד החינוך.

ייתכן כי מידע רגיש על אודות תלמידים (או מידע המסגיר מידע שכזה), עשוי להישמר במערכות האמורות ואף להיות "מועבר" במסגרתן להורים ולתלמידים.

לדוגמה, **במסגרת כתיבת הערות להורים בדבר היעדרות תלמיד או עדכון בדבר בעיות משמעת שלו במערכת לניהול פדגוגי, עלולים מורים לציין היבטים הנוגעים לסוגיות רפואיות הנוגעות לתלמיד (כדוגמת בעיות קשב וריכוז, התייחסות לטיפול תרופתי כזה או אחר, וציון סוג הרופא המטפל בתלמיד), לעניינים הנוגעים למיניותו או למגדר של התלמיד, וכדומה.**

אי-שליטת תלמידים והורים על המידע

כאמור, חלק מהמערכות לניהול פדגוגי מעניקות להורים ולתלמידים גישה לצפייה מרחוק במידע על אודות התלמידים, כגון מידע על התנהגותם והישגיהם. משמעות הדבר היא שמידע רב על אודות תלמידים עולה לרשת באופן המאפשר גישה אליו מרחוק, וזאת מבלי לקבל את הסכמתם של התלמידים ואף לא את עמדתם העקרונית ביחס לכך. **מצב עניינים זה, והפגיעה באלמנט השליטה של תלמידים על מידע הנוגע אליהם, עשויים להיתפס על-ידי תלמידים כפגיעה בפרטיותם.** דבר זה עשוי להיות רלוונטי במיוחד כאשר השימוש במידע והעברתו נעשים באופן ובמידה שאינה מחייבת זאת, קרי כשאין מדובר במצבים ייחודיים או קיצוניים שבהם ברור כי יש ליידע הורים על התנהלות הקשורה לילדיהם (כגון מעורבות תלמידים באירועי אלימות וכדומה).

דוגמה לדברים אלו ניתן לראות בעמדת הוועדה לבחינת קשרי מורים-הורים בסביבה משתנה, שבהתייחסותה לשימוש מוסדות חינוך במערכת המשו"ב להעברת מידע על אודות תלמידים להוריהם, ציינה כי: "יש חשש שהשימוש במערכת זו יעורר רתיעה בקרב מתבגרים, העלולים לפרש אותו כחדירה לפרטיותם ופגיעה בה... המתבגר עלול לראות בעין רעה את עצם הקיום וההעברה של מידע כזה, כי הוא עלול לפרשו כחשיפה של מידע אישי ללא רשותו".[44]

מצב עניינים זה עלול גם ליצור תחושה בקרב תלמידים כי כל מידע על אודותיהם - לרבות מידע הנובע מהתנהלותם במרחב הבית-ספרי - מתועד, נשמר ומועבר הלאה, באופן שאינו מאפשר להם מרחב פרטי ואישי.

44 | **בין הורים למורים בחינוך העל-יסודי – תמונת מצב והמלצות** 76-77 (ציפורה שכטמן ועודד בושריאן עורכים, 2015). הוועדה המליצה כי מידע הקשור להישגים לימודיים ולנוכחות לא יגיע ישירות להורים אלא בצורה מתווכת על ידי המתבגר, כדי שיוכל להכין את עצמו לשיחה ולדעת באיזה מידע מדובר.

דגשים והמלצות

לאור האמור, מבקשת הרשות להגנת הפרטיות להדגיש את הנקודות הבאות:

- ככלל, על מוסדות חינוך לפעול בהתאם להוראות הדין והנחיות משרד החינוך בכל הנוגע לאבטחת המידע השמור במערכות טכנולוגיות לניהול פדגוגי. כפי שצוין קודם לכן, על פי הנחיות משרד החינוך, מידע מוגן על אודות תלמידים, כמשמעותו בחוק הגנת הפרטיות, יש לשמור אך ורק במקומות המתאימים לכך.[45]
- חשוב ביותר שמשרד החינוך ינסח הנחיות ברורות בדבר התנהלות מוסדות חינוך בכל הנוגע לשימוש במערכות לניהול פדגוגי מבוסס נתונים - לרבות כאלו המאפשרות להורים ותלמידים גישה למידע - תוך השמת דגש על עניינים הנוגעים לפרטיות תלמידים, לרבות ביחס לסוג המידע שניתן לאסוף ולחשוף במסגרתן.[46]
- בהיעדר הנחיות שכאלו מומלץ שמוסדות חינוך ובעליהם ינחו את עובדי ההוראה המשתמשים במערכות לניהול פדגוגי, ובמיוחד אלו המאפשרות גישה מרחוק למידע, לשקול בכובד ראש את סוג ואופי המידע אותו הם שומרים וחושפים במסגרתן.

ככלל, מומלץ כי בטרם שמירת מידע על אודות תלמידים במערכות לניהול פדגוגי ייבחן האם קיים צורך בשמירת המידע במערכות האמורות.

כלל האצבע שמומלץ בעניין זה הוא כי כל מידע העשוי להתפרש כמידע רגיש (או כזה הניתן להסיק ממנו פרט רגיש על אודות תלמיד) יישמר רק בנסיבות המחייבות זאת, וככל האפשר רק במערכות ייעודיות המאושרות על-ידי משרד החינוך, ואשר אינן מאפשרות גישה מרחוק למידע.

עוד מומלץ שמידע רגיש על אודות תלמיד (כגון מידע רפואי, מידע הנוגע לזהותו המגדרית או הנוגע למיניותו) לא יועלה למערכות לניהול פדגוגי המעניקות הרשאות לגישה "מרחוק" להורים ולתלמידים, אלא אם ניתנה הסכמת ההורים לכך, ותוך מתן משקל לעמדת התלמיד בנושא (ככל שהביע את עמדתו). במידה שהורים מסרבים להעניק הסכמתם – מומלץ כי העברת המידע הרגיש תיעשה שלא באמצעות הרשת.[47]

45 | ראו מסמך "מדיניות שמירה וטיפול במידע מוגן במוסדות חינוך", לעיל ה"ש 4.

46 | למיטב ידיעת הרשות, בימים אלו מצוי משרד החינוך בשלבי גיבוש חוזר מנכ"ל בנושא.

47 | יובהר כי ככלל, לגישת הרשות להגנת הפרטיות, מידע על אודות ציונים, חיסורים, איחורים והתנהגות שאינה תואמת את כללי המשמעת במוסד החינוכי אינו מסוג המידע המצריך את הסכמת ההורים לצורך העברתו במסגרת מערכות לניהול פדגוגי וניהול למידה המאפשרות גישה מרחוק למידע.

- בהתאם לעקרון צמידות המטרה והצורך בצמצום מידע, בנסיבות בהן מידע על אודות תלמידים מועלה למערכות לניהול פדגוגי ונשמר בהן, מומלץ שמוסדות חינוך והבעלויות עליהם יבחנו את הצורך בהמשך שמירת כלל המידע לאורך זמן, וכן ימנעו משמירת מידע עודף שאינו נדרש למטרת איסופו ולמטרת המאגר.[48]

ח.4| למידה מרחוק[49]

בשנים האחרונות עוברת מערכת החינוך תהליכים להטמעת השימוש ביישומים ללמידה מרחוק, בעיקר כמענה לצורך בקיום לימודים בעתות משבר. למידה מרחוק (או למידה מקוונת) היא מסגרת של למידה הנערכת באופן מקוון ומאפשרת לתלמידים הנמצאים מחוץ לכותלי המוסד החינוכי להשתתף בשיעורים המועברים על-ידי מורים, בזמן אמת או באופן מוקלט. למידה זו מתבצעת באמצעות יישומים ללמידה סינכרונית, כגון מערכות Microsoft Teams, Zoom ו- Skype. בעת התמודדות מערכת החינוך עם נגיף הקורונה השתמשו מוסדות חינוך בתוכנת זום להעברת שיעורים באופן מקוון לתלמידים בכל השלבים החינוכיים הרשמיים, מגילאי גן ועד גילאי תיכון.

למידה מרחוק מהווה חלק מהלמידה ההיברידית, המשלבת בין למידה מקוונת מרחוק ולמידה פרונטאלית בכיתה. למידה מרחוק יכולה להתקיים באופן סינכרוני שבו התלמידים והמורה מתקשרים זה עם זה באופן מקוון ובזמן אמת, או באופן א-סינכרוני, שבו פעילות הלימוד בין המורה לתלמידים מתקיימת במועדים שונים.

למציאות של שימוש תלמידים ביישומים ללמידה מרחוק עשויה להיות השלכה דרמטית על פרטיותם, לרבות מבחינת ההגנה על מידע אישי הנוגע אליהם. יישומים דיגיטליים ללמידה מרחוק עשויים לאסוף או לחשוף מידע על תלמידים, לרבות מידע רגיש, כגון נתונים הנוגעים לזהות התלמידים. שימוש ביישומים האמורים עשוי להביא גם לאיסוף או לחשיפת מידע הנוגע לתלמידים שאינו נובע ישירות מהתהליך הלימודי, כגון מידע על אודות הרגלי הגלישה של התלמידים וכתובות מגוריהם. **מידע זה עלול להיות מועבר לגורמים שלישיים, כגון חברות מסחריות, העשויות להשתמש בו למטרות שונות.**

בנוסף, יישומים דיגיטליים ללמידה מרחוק, כמרבית המערכות המקוונות, אינם חסינים מפני חדירה ומפני מצבים של דלף מידע. מצב זה עשוי להביא לכך שמידע רגיש רב על

48 | לעניין זה ראו לדוגמה תקנה 2(ג) לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, וכן טיוטת מסמך צמצום המידע, לעיל ה"ש 23.

49 | חלק זה מבוסס על הנחיות משרד החינוך שפורסמו בנושא ועל מסמך "הגנת פרטיות תלמידים בלמידה מרחוק: דגשים והמלצות להתנהלות בתקופת התמודדות עם נגיף הקורונה" שפרסמה הרשות לקראת פתיחת שנת הלימודים תשפ"א, לעיון במסמך ראו: https://www.gov.il/BlobFolder/reports/privacy-back-to-school-digital/he/learning.pdf. ככל שיפורסמו הנחיות נוספות בנושא מטעם משרד החינוך, המדריך יעודכן לאורן.

אודות תלמידים עשוי להיחשף, לדלוף ולהגיע לידי גורמים שיעשו בו שימוש לרעה. חשיפה שכזו עשויה להיגרם גם כתוצאה מפעילות גורמים אחרים המקיימים אינטראקציות עם תלמידים על גבי היישומים האמורים, כגון תלמידים אחרים, מורים ומרצים.

מצב זה רלוונטי במיוחד בנוגע לילדים, ובעיקר לכאלו שבגילאים צעירים. ילדים, ובמקרים רבים גם הורים האמונים על ההגנה עליהם, אינם מודעים לסוגיות הנוגעות לשימוש גורמים שונים (מסחריים ואחרים) במידע אישי הנוגע לילדים, ולהשלכות שימוש זה על חייהם ועתידם.

לפיכך, ילדים נחשבים מטרה נוחה לגורמים מסחריים (ואחרים), שאיסוף מידע מהווה רכיב מרכזי בפעילותם. יש לזכור כי ככלל, ילדים מודעים פחות לניסיונות "לדוג" מידע הנוגע אליהם, וכן כי ילדים נוהגים לא פעם לחשוף ברשת מידע הנוגע אליהם או אל בני משפחתם, מבלי לתת את הדעת לכלל ההשלכות הנובעות מחשיפתו, ובאופן העשוי לפגוע בהם ובעתידם.

פגיעה שונה בפרטיות עשויה להתרחש גם כתוצאה מעצם החשיפה הפיזית של תלמידים במסגרת היישומים השונים. כך לדוגמה, לאור חיוב תלמידים במוסדות חינוך מסוימים "לפתוח" את מצלמות הרשת שלהם במסגרת שיעורי הזום שנערכו בתקופת ההתמודדות עם נגיף הקורונה, עלו טענות מצדם של תלמידים כי חיוב זה פוגע בפרטיותם. התלמידים טענו בעניין זה, בין היתר, כי חובה זו חושפת בפני כל חלקים מן המרחב הפרטי שלהם בניגוד לרצונם, וכן הביעו חשש כי יצולמו במסגרת השיעורים על-ידי תלמידים אחרים וכי תמונות אלו יופצו ברשתות חברתיות, ללא הסכמתם. הנושא מצוי כיום בהליכי הסדרה על-ידי משרד החינוך,[50] **ויובהר כי לא ניתנה הנחיה לחייב פתיחת מצלמות על ידי משרד החינוך.**

למידה סינכרונית - דגשים והמלצות כלליים

להלן פירוט דגשים לגורמים המבקשים להפעיל תוכניות ללמידה סינכרונית מרחוק לתלמידים באמצעות שימוש ביישומים ללמידה סינכרונית של חברות חיצוניות. הקפדה על דגשים אלה עשויה למזער את אפשרות הפגיעה בפרטיות המשתמשים במסגרת תהליכים של למידה מרחוק:

- בעת הליך בחינת ובחירת זהות היישום ללמידה סינכרונית מומלץ כי ייבחנו היבטים של הגנה על פרטיות ומידע, וכי שיקולים של אבטחת מידע יהוו שיקולים מרכזיים בהליך בחירת סוג וזהות היישום בו אתם מבקשים לעשות שימוש.

50 | סוגיית חיוב תלמידים בפתיחת מצלמות במהלך שיעורים נמצאת כיום בהליכי הסדרה במסגרת הנחיות משרד החינוך. עם פרסום הנחיות אלו יעודכן המדריך לאורן. ככלל, ככל הידוע לרשות, משרד החינוך רואה חשיבות רבה בשימוש בווידאו ובשמע על ידי התלמידים במסגרת הלמידה הסינכרונית. עניין זה נועד לחזק את הקשר בין המורה לתלמיד בהיבט הלימודי והרגשי ולאפשר הבנה של תהליך הלמידה. בכל הנוגע למצבים בהם תלמידים יעדיפו שלא להפעיל מצלמה – עמדת משרד החינוך, ככל הידוע לרשות, היא כי התייחסות למצבים אלו תלווה בשיח משותף עם התלמיד, הוריו והמורה.

בכל הנוגע לשימוש ביישומים ללמידה סינכרונית במסגרת פעילות מוסדות חינוך – מומלץ כי מוסדות חינוך ו/או רשויות מקומיות המבקשים להשתמש ביישומים האמורים יפעלו מול הגורמים הרלוונטיים במשרד החינוך על מנת לוודא כי היישום בו הם מבקשים לעשות שימוש ללמידה סינכורנית מאושר על-ידי המשרד, וכי הוא עומד בהקשר זה בכל כללי אבטחת המידע הנדרשים ע"פ הוראות הדין.

כך לדוגמה, בבחירה בין יישומים המציעים כלים דומים ללמידה מרחוק, מומלץ כי ייבחר היישום המשתמש באמצעים המשמעותיים והנרחבים יותר להגנה על מידע (כגון הצפנה מקצה לקצה לשיחות הווידאו), וכן כזה המחזיק במסמך מדיניות הפרטיות המפורט יותר. במובן זה, שימוש של יישום בשירותים של חברת הגנת מידע מוכרת ובעלת רקע מוכח בטיפול באירועי אבטחת מידע, עשוי להוות יתרון בהליך בחירת היישום.

- מומלץ כי השימוש ביישומים ללמידה סינכרונית יעשה במסגרת של רכישת רישיון לשימוש ביישומים אלו. במובן זה מומלץ להימנע מלדרוש מתלמידים ועובדי הוראה להשתמש בגרסאות "חינמיות" של יישומים אלו.
- ביישומים בהם מתקיימים שיעורים בזמן אמת מומלץ לעשות שימוש בהגדרות היישומים השונים לחיזוק ההגנה על פרטיות התלמידים. כך לדוגמה, ביישומים הרלוונטיים, יש להגדיר כי זהות המשתתפים בשיעורים המקוונים תוגבל רק לתלמידי הכיתה, להגדיר חובת רישום סיסמה בעת כניסה לשיעורים, להגדיר כי כניסה לשיעור תעשה רק לאחר המתנה ב"חדר המתנה" ואישור המורה, נעילת השיעור לאחר כניסת כל התלמידים או לחילופין שימוש בפונקציה המתריעה על כניסה של משתמש חדש לשיעור וכדומה.

  כך לדוגמה בתוכנת זום, על מנת לפקח על המצטרפים המורשים לישיבה יש לסמן את האפשרות Enable Waiting Room לשם שימוש ב-"חדר המתנה", ולאחר הצטרפות כלל המשתתפים יש לבחור Lock Meeting לנעילת הפגישה מפני לא אורחים לא קרואים. ובנוסף, לשם הגנה על המשתתפים מומלץ לוודא שאפשרות העברת קבצים File Transfer כבויה.
- ביישומים בהם מתקיימים שיעורים בזמן אמת מומלץ לשלוח לתלמידים את הקישור לשיעורים באמצעי אחד מוגדר קבוע ומוסכם מראש על כל התלמידים , בו ניתן לוודא את זהות הנמען (הודעת טקסט למספר טלפון של התלמיד/הורה התלמיד, שליחת מייל לחשבון הדוא"ל של הורה התלמיד וכדומה). אפשרות חלופית היא שהקישור לשיעור יפורסם במערכת המקוונת הבית-ספרית.
- מומלץ כי אפשרות הקלטת השיעור תהיה מוגבלת רק למארח ולא ליתר המשתתפים בשיעור, וכי הקלטה כזו תעשה רק במידה והדבר חיוני לצרכי המוסד (כגון מתן אפשרות

לתלמידים נעדרים לחזות בשיעור בהמשך). אם השיעור מוקלט – יש ליידע את המשתתפים על הקלטתו, ולוודא כי משלוח הקישור לשיעור המוקלט תעשה רק למורשים הנדרשים לצפות בשיעור המוקלט וכן לקבוע סיסמה לשם צפייה בשיעור המוקלט.

- מומלץ כי שמירת החומרים המצולמים במסגרת השיעורים תיעשה במחשבים מקומיים או לכל הפחות בחשבונות "ענן" מאובטחים וייעודיים (כגון זה של Microsoft 365) שאושרו על-ידי משרד החינוך. בכל מקרה רצוי שלא לשמור את החומרים בחשבונות המנוהלים

- מומלץ כי עם המעבר למסגרת של למידה מרחוק יובהרו ויחודדו למשתמשים ביישומים, לרבות תלמידים ועובדי ההוראה, הכללים השונים הנוגעים להתנהלות במסגרת יישומים אלו, לרבות בנוגע להגנה על הפרטיות, וזאת כדוגמת הכללים שפורטו בחלק הקודם למסמך זה.

- בנוגע לחיוב תלמידים לפתוח מצלמות במסגרת שיעורים ובחינות – בהיעדר הנחיה אחרת של משרד החינוך רצוי שמוסדות החינוך והגורמים הרלוונטיים השונים יבחנו ויעמידו בעת הצורך חלופות שיאפשרו למורים לבדוק נוכחות תלמידים בשיעורים ולשמור על טוהר הבחינות, בדרכים שפגיעתן בפרטיות תלמידים היא הפחותה ביותר.

  לדוגמה, ניתן לקבוע שפתיחת מצלמות בשיעורים תעשה באופן מדגמי או בנקודות זמן מסוימות (כגון בתחילת השיעור ובסופו), לקיים דיונים עם תלמידים במסגרת השיעורים, וכן לבקש מתלמידים להגיב בעל-פה או בכתב על נושאים שנלמדו בשיעורים, באופן שיעיד אם הם נכחו בשיעורים והקשיבו לנלמד בהם. בנוגע לבחינות ניתן לבחון אפשרות של המרתן בהגשת עבודות, ככל שהדבר ניתן ונכון מבחינה לימודית/פדגוגית. בכל מקרה רצוי שלמנהלים ולמורים יעמוד גם שיקול דעת בנושא, אשר יאפשר להם, בנסיבות מיוחדות, להתיר לתלמידים המבקשים זאת, שלא לפתוח מצלמות בשיעורים. כיבוד פרטיות תלמידים עשוי בהקשר זה, כמו בהקשרים אחרים, להוות גם בסיס לכינון וחיזוק יחסי אמון. על כן הרשות ממליצה כי המוסד והצוות החינוכי יאפשרו לתלמידים להביע את דעתם ולהשמיע את קולם בנושא. כאמור, נושא זה מצוי כיום בהליכי הסדרה על-ידי משרד החינוך, וכי נכון למועד כתיבת המדריך לא ניתנה הנחיה מטעם משרד החינוך לחיוב תלמידים בפתיחת מצלמות.

- רצוי כי מוסדות חינוך, וגורמים שמוסדות אלו נמצאים בבעלותם, ישקלו לרכוש במרוכז אמצעים לכיסוי מצלמות (במחשבים ובטלפונים חכמים) אשר יועברו לשימוש תלמידים.

- מומלץ להגביר את המודעות ולחדד את הכללים הרלוונטיים ביחס לאופן השימוש במידע והגנתו מול עובדים במוסד החינוכי העשויים להיחשף למידע. בעניין זה רצוי להדריך עובדים במוסד (לרבות עובדי הוראה, מזכירות והנהלה) בדבר הפעולות שעליהם

שעליהם לבצע על מנת להקטין סיכון להתקיימות אירועי אבטחת מידע ופגיעה בפרטיות.[51]

- מומלץ שמוסדות חינוך יפעלו להנגשת ולהטמעת ההמלצות להגנה על פרטיות ולהתנהלות מיטבית ובטוחה ביישומים השונים ללמידה סינכרונית, אשר פורטו קודם לכן, בקרב תלמידים והורים.[52] מודעות לסוגית הפרטיות היא קריטית לשם ההגנה עליה.
- מומלץ לעשות שימוש בכלים הנלווים המסופקים עם היישומים על מנת לנטר את השימוש ביישומים אלו, לשם איתור ניסיונות שימוש לרעה במערכת (כגון ניסיונות "דיוג") ובחינת אופן התנהלות תלמידים ועובדי הוראה ביישומים. מומלץ להגדיר את המערכות בצורה אשר תגביר את אבטחת המידע בסוגיות כגון אופן ההזדהות, ותאפשר לאתר שימושים לא מורשים. כמו כן, לאור העלייה בהיקף השימוש ביישומים ללמידה סינכרונית מומלץ להגביר את הניטור והפיקוח על פעילות היישומים והחברות במסגרתם הם פועלים, וזאת בין היתר בכל הנוגע לעמידה בכללי אבטחת מידע. על סוגיה זו יורחב בהמשך הפרק.

הגנת הפרטיות במסגרת למידה משולבת[53]

כאמור, למידה מרחוק כוללת גם אפשרות של למידה משולבת (או היברידית), במסגרתה מצולם שיעור המתקיים בכיתה בזמן אמת ללא נוכחות פיזית של התלמידים או נוכחות חלקית שלהם, שיתר התלמידים משתתפים בשיעור מרחוק. להלן יצוינו מספר כללים ודגשים ספציפיים בהקשר זה:

- בגני ילדים אין לקיים למידה משולבת בנוכחות ילדים. למידה משולבת יכולה להתקיים במקרה בו הגננת מלמדת בגן ללא נוכחות פיזית של ילדים בתוך מבנה הגן. עם זאת, לאור הנחיות משרד החינוך האוסרות על הצבת מצלמה קבועה בתוך מבנה גן הילדים, במקרה שכזה הצילום יכול להתבצע רק באמצעות מצלמת המחשב בו עושה הגננת שימוש או באמצעות המצלמה שבמכשיר הטלפון של הגננת.

51 | להרחבה בנוגע להיבטים של הגנה על פרטיות בהפעלת מדיניות של עבודה מרחוק ראו https://www.gov.il/BlobFolder/reports/corona_work/he/WORK%D6%B9PRIVACY%D6%B9CORONA.pdf.

52 | למיטב ידיעת הרשות, משרד החינוך מפעיל תכנית מערכתית להתנהלות מיטבית ברשת, הכוללת גם התייחסות להיבטים של שמירת הפרטיות. ראו https://cms.education.gov.il/EducationCMS/Units/Shefi/Hitnahalut_Mitavit_Bareshet/.

53 | חלק זה מבוסס על הנחיות משרד החינוך בנושא "הנחיות להעברת שיעור המתקיים בכיתה לתלמידים הלומדים מרחוק בתקופת הקורונה (למידה משולבת)" מחודש נובמבר 2020, https://poh.education.gov.il/PniotVemokdeiSherut/Pages/hybrid-class.aspx. בימים אלה נבחנת במשרד החינוך מדיניות המאפשרת למידה משולבת גם בגני ילדים.

- צילום שיעור בזמן אמת בבתי-ספר במסגרת למידה משולבת נועד אך ורק לשם העברת השיעור לתלמידים שאינם נוכחים בכיתה. אין לעשות במצלמות או בחומרי הצילום כל שימוש אחר.
- המצלמות יופעלו אך ורק בזמני השיעורים ולא בזמנים אחרים, כגון בהפסקות.
- במסגרת למידה משולבת בבתי-ספר, צילום השיעור בזמן אמת מותנה בהסכמת המורה.
- חל איסור על צילום התלמידים הנוכחים בכיתה במסגרת השיעור. על המורה לוודא, עם תחילת כל שיעור, כי המצלמה בה הוא משתמש אינה מכוונת לכיוון התלמידים אלא לכיוונו.
- טרם פתיחת המצלמה בתחילת השיעור יציין המורה בפני התלמידים הנוכחים בכיתה כי השיעור מצולם ומעובר לתלמידים הלומדים מרחוק. כמו כן, על המורה להבהיר לתלמידים כי קולם עשוי להישמע ולהיות מוקלט. כפי שכתוב בהנחיות משרד החינוך בנושא, מטרת הדגשת מידע זה נועדה להגביר את המודעות של התלמידים לשידור ולאפשר להם לבחור באיזו מידה להשמיע את קולם.
- בסיום השיעור על המורה להפסיק את הצילום ולוודא את כיבוי האפליקציה שבה השתמש להעברת המידע לתלמידים הלומדים מרחוק.
- על מורים להפעיל שיקול דעת בנוגע לצילום שיעורים בהם מתקיים שיח רגיש ומורכב, כדוגמת שיעורי חינוך מיני). אם במהלך השיעור מתעורר חשש שתלמיד עלול לחשוף מידע רגיש שעלול לפגוע בפרטיותו – על המורה לבקש לקיים עמו שיח אישי ונפרד, מחוץ לשיעור המצולם.
- חל איסור על תלמידים או הוריהם לצלם, להקליט או להפיץ את השיעור המצולם.
- ככלל, אין לשמור צילום או הקלטה של שיעור. עם זאת, במקרים חריגים בהם קיים צורך לשמור צילום/הקלטת שמע לשם העברת השיעור לתלמידים אשר לאור נסיבות מוצדקות לא יכלו לצפות בשיעור בזמן אמת, מורה רשאי לשמור את הקלטת השיעור, וזאת לשם העברתה לתלמידים האמורים. במצב עניינים זה על המורה להפקיד על כללים שונים הנוגעים לאבטחת המידע. כך לדוגמה, על המורה לוודא כי הקישור לשיעור יישלח רק למורשים לצפות בו; על המורה לקבוע סיסמה לשם צפייה בשיעור המוקלט; שמירת החומרים המוקלטים תיעשה אך ורק במחשבים מקומיים שהותקנו בהם אמצעי הגנה ואבטחת מידע או בשירותים מאובטחים וייעודיים שאושרו על-ידי משרד החינוך; העברת הקישור להקלטה תיעשה באמצעים מקובלים ותוך שימוש במערכות מאובטחות ומוצפנות להעברת מידע, אשר אושרו על-ידי משרד החינוך.
- המורה ימחק את ההקלטה עד שבוע ימים מיום העברת ההקלטה, לכל המאוחר.

כללי אבטחת מידע במסגרת תהליכי למידה מרחוק באמצעות יישומים טכנולוגיים

כל גורם, ציבורי או פרטי, שבבעלותו מאגר מידע כהגדרתו בחוק הגנת הפרטיות מחויב על פי דין בעמידה בכללים שונים הנוגעים לאבטחת המידע שבמאגר. כללים אלו מפורטים בחוק הגנת הפרטיות ובתקנות שהותקנו מכוחו, לרבות תקנות אבטחת מידע.

התקשרות גורמים ציבוריים ופרטיים (שהם בעלי מאגרי המידע) עם חברות חיצוניות לשם שימוש ביישומים טכנולוגיים לקיום מערך למידה מרחוק, הכרוך במתן גישה למאגרי המידע, מהווה פעולה של מיקור חוץ, כמשמעה בתקנה 15 לתקנות אבטחת מידע.[54] התקשרות זו מחייבת את בעל מאגר המידע בעמידה בכללי אבטחת מידע ספציפיים. כך, בעל מאגר מידע מחויב, בין היתר:

- לבחון, לפני ביצוע ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות זו.
- לקבוע מפורשות בהסכם עם הגורם החיצוני כללים הנוגעים לאופן השימוש של הגורם החיצוני במידע שבמאגר, לרבות ביחס למטרות השימוש במידע, סוג העיבוד במידע שהגורם החיצוני רשאי לעשות, משך ההתקשרות וכן אופן יישום הגורם החיצוני את החובות מתחום אבטחת המידע החלות עליו.
- לנקוט אמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם בכלל ובהוראות תקנות אבטחת מידע, בפרט.

לאור כל האמור, על גורמים המבקשים להשתמש ביישומים טכנולוגיים להפעלת מערך למידה מרחוק לוודא כי הם עומדים בהוראות הדין בהקשר זה, ולפעול לפיהן. כמו כן, ככל שגורמים מבקשים לעבוד עם יישומים של למידה מרחוק השומרים את המידע הנאסף במסגרתם במאגרי מידע המוחזקים מחוץ לגבולות מדינת ישראל, יש לוודא גם עמידה בהוראות תקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001.

עד כאן פורטו הדגשים וההמלצות העקרוניות של הרשות להגנת הפרטיות בנושא. יצוין כי אתר משרד החינוך כולל מידע רב בנושא הלמידה מרחוק, לרבות פירוט מדיניות המשרד בנושא, פירוט דגשים פדגוגים ללמידה מרחוק בעת סגר, וכן פירוט המלצות ספציפיות בנושא אבטחת מידע והגנת פרטיות ביישומים השונים ללמידה מרחוק.[55]

54 | הרשות להגנת הפרטיות פרסמה מספר המלצות לנושאים אותם ראוי לענן בחוזה בין בעל מאגר המידע לגורם החיצוני איתו הוא מתקשר לצורך יישום תקנה 15 לתקנות אבטחת המידע. לעניין זה ראו: https://www.gov.il/he/departments/general/data_security_outsourcing.

55 | https://pop.education.gov.il/sherutey-tiksuv-bachinuch/virtual-classroom-meeting/; https://docisolation.prod.fire.glass/?guid=2e5a68ff-5555-4131-be03-9cba5072515f

ח.5 | שימוש באמצעים דיגיטליים שאינם ייעודיים

תופעה מרכזית המתפתחת בשנים האחרונות במערכת החינוך היא שימוש עובדי מוסדות חינוך (צוותי הוראה, סגל מינהלי וכו') באמצעים דיגיטליים שאינם ייעודיים לאיסוף והעברת מידע, וזאת כחלק ובמסגרת עבודתם.

עובדי מוסדות חינוך משתמשים לא פעם באמצעים דיגיטליים לא ייעודיים לשמירת מידע על אודות תלמידים, ולהעברתו. תחת אמצעים אלו ניתן למצוא מכשירי טלפון חכמים, טאבלטים ומחשבים ניידים-אישיים, וכן תוכנות ואפליקציות פרטיות להעברת מידע המותקנות בטלפונים ובמחשבים הפרטיים של העובדים, כגון WhatsApp ו-Gmail. לזאת יש להוסיף גם צוותי הוראה שבמסגרת ההוראה שלהם משתמשים בתוכנות "חינמיות" שלא אושרו לשימושים מסוימים במערכת החינוך, ושבמסגרתן עלול להיאסף מידע על אודות תלמידים, כגון: Kahoot, Google maps, YouTube ועוד.[56]

מצב זה עלול, בשימוש לא מותאם, לפגוע בפרטיות תלמידים באופנים הבאים:

- אמצעים שאינם ייעודיים עלולים להיות בלתי מספקים מבחינת אבטחת מידע. שמירת מידע על אודות תלמידים במכשירים או תוכנות שאינם מאובטחים דיים, וכן העברתו באופן מקוון שאינו מאובטח דיו, עלולים להביא לזליגתו ולחשיפתו של המידע. מצב זה עלול להיווצר בין כתוצאה מפריצה מכוונת לאותם אמצעים ותוכנות, ובין כתוצאה מכשל פנימי בהם.
- חשיפת מידע על אודות תלמידים עלולה להתרחש גם כתוצאה מטעויות אנוש. ערבוב השימוש באמצעים השונים - הן לצרכי עבודה והן לצרכים אישיים - מגבירים את הסיכון שמידע על אודות תלמידים השמור במכשירים של עובדי המוסד החינוכי ובתוכנות עימן הם עובדים, יועבר בטעות לגורמים שונים. החשיפה עלולה להתרחש גם במסגרת החלפת המכשיר בו שמור המידע, או תיקונו.
- שמירת והעברת מידע על אודות תלמידים באמצעים שאינם ייעודיים עלול להביא לכך שחברות מסחריות שאמצעים אלו נמצאים בבעלותם ישתמשו במידע לצרכיהן. חשש זה הוא קריטי בעיקר ביחס לתוכנות ואפליקציות "חינמיות" שהמודל הכלכלי שלהן מבוסס על מתן שירותים ללא עלות כספית בתמורה לאיסוף ועיבוד המידע הנשמר והמועבר באמצעותן.

56 | אלו דוגמאות בלבד. בכל מקרה אין בדברים בכדי לטעון כי עצם השימוש בתוכנות אלו ואחרות הוא פסול, אלא כי שימוש זה צריך להיעשות בהתאם להנחיות משרד החינוך, ותוך מתן התייחסות להיבטים של פרטיות תלמידים.

- שימוש עובדי הוראה עם תוכנות שאינן ייעודיות במסגרת לימודית עלול להביא לכך שגם תלמידים ידרשו להשתמש בתוכנות אלו, על כל המשתמש מכך מבחינת איסוף מידע על אודותיהם.

להלן מספר דגשים והמלצות כלליות להתנהלות עובדי מוסדות חינוך בנושא:

- כפי שצוין קודם לכן במדריך, על פי הנחיות משרד החינוך, מידע מוגן על פי חוק הגנת הפרטיות (ובכלל זה נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו)[57] יש לשמור רק במערכות מאושרות, ולא במחשבים פרטיים או חשבונות ענן פרטיים.

לאור האמור, על עובדי מוסדות חינוך להימנע מלהעביר מידע מוגן על אודות תלמידים באמצעות אמצעים שאינם ייעודיים לכך, כגון חשבונות דוא"ל פרטיים או אפליקציות מסחריות להעברת מסרים מידיים.

- בכל הנוגע למידע לא מוגן כהגדרתו בהנחיות משרד החינוך - ככלל, הרשות ממליצה לכלל הגורמים הפועלים במסגרת מערכת החינוך להימנע ככל הניתן גם מהעברת מידע שכזה באמצעות אמצעים דיגיטליים שאינם ייעודיים, ולעשות שימוש אך ורק באמצעים המאושרים על-ידי משרד החינוך.

- **לגישת הרשות, בנסיבות בהן לא קיימת חלופה סבירה ויעילה להעברת מידע שאינו מוגן להורים ולתלמידים אלא באמצעות אמצעים שאינם ייעודים, ובמידה והדבר אינו סותר את הנחיות משרד החינוך בנושא – שימוש זה הוא אפשרי, אך מומלץ שתתקבל הסכמת הורים להעברת המידע באמצעות אמצעים אלו.**

- במידה ונעשה שימוש באמצעים שאינם ייעודיים להעברת מידע שאינו מוגן על אודות תלמידים מומלץ למחוק את המידע מזיכרון האמצעי בו נעשה שימוש, אלא אם ניתן להצביע על סיבה מיוחדת לשמירת עותק מהמידע גם במכשיר.

- מומלץ כי מידע לא מוגן על אודות תלמידים, שנשמר והועבר במסגרת שימוש באמצעים שאינם ייעודיים, לא יישמר במקביל גם בשירותי גיבוי ענן פרטיים, כגון Google Drive או Dropbox. במידה והמידע נשמר בשירותי ענן שכאלו – יש למחוק את המידע משירותים אלו בהקדם האפשרי.

57 | לפירוט עמדת הרשות להגנת הפרטיות בנושא הגדרת "מידע" על-פי חוק הגנת הפרטיות, ראו מסמך "גילוי דעת: מהם 'מידע' ו'ידיעה על ענייניו הפרטיים של אדם' בחוק הגנת הפרטיות", לעיל ה"ש 3.

- בהתאם לגישת צמצום המידע, מומלץ שבעת שימוש באמצעים שאינם ייעודיים יועבר אך ורק המידע המינימלי הנדרש למטרת העברתו ושמירתו.
- במקרה של רצון לעשות שימוש באמצעים שאינם ייעודיים ושלא אושרו על-ידי משרד החינוך (לדוגמה, כחלק מתהליך הלמידה), על מנהל המוסד החינוכי לבדוק את בטיחות השימוש באמצעי. בעניין זה מומלץ למוסד החינוכי לרכוש מנוי עבור המשתמשים.
- בטרם עשיית שימוש באמצעי שלא אושר על-ידי המשרד יש לבחון האם קיימת חלופה הולמת לאמצעי זה במסגרת האמצעים המאושרים על-ידי המשרד.
- בעת שימוש עובדי הוראה בתוכנות "חינמיות" שאינן ייעודיות ושאינן מאושרות על-ידי משרד החינוך (קרי שאין מדובר בספקים מאושרים) כחלק ובמסגרת מתהליך הלמידה, יש להימנע מלדרוש מתלמידים לפתוח חשבון משתמש בתוכנות אלו או להתקין אפליקציות של תוכנות אלו במכשיריהם. ככל שלדעת הגורם החינוכי יש חשיבות פדגוגית בשימוש בתוכנות שכאלו, יש להבהיר לתלמידים כי הם אינם מחויבים להוריד את התוכנות וכי הדבר נתון לבחירתם. כמו כן, במצב שכזה, ראוי כי הגורם החינוכי ינצל את ההזדמנות על מנת לדון עם התלמידים בהיבטים של שימוש במידע על אודותיהם על-ידי תוכנות שכאלו, וכן ינחה את התלמידים שהורידו את התוכנות לצרכי השיעור, למחוק אותן לאחר סיום המשימה הלימודית.
- על הגורם החינוכי להקפיד שלא להעלות מידע אישי (כגון כתובת או מספר תעודת זהות) שלכם או של תלמידיכם לאמצעי דיגיטלי שאינו מאושר על-ידי המשרד. יש להנחות גם את התלמידים להימנע מלחשוף מידע אישי (שלהם או של חבריהם) במסגרת שימושם בכלים אלו.
- על הגורם החינוכי להקפיד שלא להנחות תלמידים להירשם לתוכנות או אפליקציות שאינן תואמות את גילם מבחינת דרישת הגיל המינימלי הקבוע בתנאי השימוש שלהן. במקרים שכאלו יש לבקש את אישור הורי התלמידים להורדת ולשימוש בתוכנה או האפליקציה.

ח.6| אמצעי קצה

שימוש תלמידים באמצעי קצה עשוי לטמון בחובו סיכונים לפרטיותם של תלמידים. סיכון אחד עלול לנבוע משימוש לא ראוי של מוסדות חינוך במחשביהם של תלמידים, וזאת לדוגמה, לצרכי אכיפת משמעת.

כך למשל, בשנת 2010, תלמיד אמריקני בן 16 תבע את מחוז בית ספרו לפיצויים בגין פגיעה בפרטיותו. התלמיד טען שבית הספר בו הוא לומד השתמש במחשב נייד שסיפק לתלמידיו וצילם, ללא ידיעתו ובאמצעות מצלמת המחשב, מאות תמונות שלו במשך שבועיים, בין היתר בעת ששהה בביתו ובחדרו הפרטי. העניין התגלה לתלמיד כשעוזרת המנהל האשימה אותו, בהתבסס על התמונות, כי התנהג בביתו באופן המעיד שהשתמש בסמים. התביעה הסתיימה בפשרה מחוץ לכותלי בית המשפט במסגרתה שולמו לתלמיד ולתובע נוסף פיצויים בסך 610,000 דולר.

שימוש מוסד חינוך באמצעי קצה למעקב אחר התנהלותם יכול להיעשות גם בדרכים אחרות, כגון בחינת אתרי האינטרנט בהם הם גולשים וזמני השימוש שלהם ברשת. כך לדוגמה, כאשר מחשב נייד שהועבר לתלמיד לשימוש זמני (לדוגמה, לשנה אקדמית) מוחזר למוסד החינוך סביר להניח שיהיה בו מידע רב אודות אופן השימוש של התלמיד במחשב, לרבות מידע על אתרים בהם גלש, שיחות אותן ניהל עם חבריו ברשת וכו'.

שימוש תלמידים באמצעי קצה עשוי לטמון בחובו סיכונים בנוגע לפרטיותם של תלמידים גם מצד של הגורם המפעיל/המספק את האמצעי. מכיוון שאמצעי הקצה מסופקים לבתי ספר מטעמן של חברות מסחריות, ייתכן כי חברות אלו עשויות לאסוף מידע על אודות תלמידים, אשר נוצר כתוצאה משימושם באמצעי הקצה, וזאת לצרכים מסחריים שלהן. כך לדוגמה, בתלונה של מכון EFF לרשות המסחר הפדרלית בארה"ב (FTC) נטען בהקשר זה, כי מחשבים שסופקו לבתי ספר מטעם חברת גוגל ואשר פעלו על מערכת Google - Chromebooks, כללו רכיב בשם "Chrome Sync", אשר אפשר לגוגל, במצב המקורי של הרכיב (default), לאסוף ולהשתמש במידע הנוגע לנתוני הגלישה של תלמידים למטרות שונות.[58]

58 | https://www.eff.org/document/ftc-complaint-google-education.

דגשים והמלצות

- על מוסדות חינוך להימנע מכל שימוש באמצעי קצה למעקב אחר התנהלות תלמידים (בזמן שעות הלימודים ומעבר להן). שימוש שכזה באמצעי הקצה, שנעשה ללא יידוע וקבלת הסכמה מצד התלמיד והוריו, הוא פסול ואינו חוקי.
- מומלץ כי בעת השבת תלמידים את אמצעי הקצה אשר היו בשימושם לרשות מוסד החינוך ימחק הגורם הרלוונטי במוסד החינוכי (או בגורם שהמוסד נמצא בבעלותו) את כל המידע שנצבר כתוצאה מפעילות התלמידים במסגרת אמצעי הקצה, אלא במקרים חריגים ביותר שיצדיקו את שמירת המידע וניתוחו, ובאישור משרד החינוך (כמו לדוגמה כאשר מתעורר חשש כי התלמיד השתמש באמצעי הקצה להפצת סרטונים בעלי אופי מיני של תלמידים אחרים וכו').
- מומלץ ליידע הורים ותלמידים המשתמשים באמצעי קצה על האפשרות שמידע אישי על אודות התלמידים ייאסף במסגרת שימושם באמצעים האמורים, וזאת על-ידי הגורמים המספקים את האמצעים והאפליקציות השונים.
- מומלץ ליידע הורים ותלמידים בדבר הצורך לאבטח את השימוש באמצעי הקצה, לדוגמה בהקשר של שימוש בסיסמאות כניסה חזקות למכשיר ובנוגע לאבטחתו באופן פיזי.
- ראוי כי מוסדות החינוך יוודאו כי הגורמים הפרטיים המספקים את אמצעי הקצה לא אוספים מידע אישי על אודות תלמידים, מעבר לנדרש לתפעול באמצעים מבחינה טכנולוגית.

נספח | ריכוז וסיכום חוזרי מנכ"ל והנחיות משרד החינוך העוסקים, באופן ישיר או עקיף, בהיבטים שונים של פרטיות תלמידים[59]

- **חוזר מנכ"ל "שימוש תלמידים באמצעי קצה לצורכי למידה"** (הוראת קבע מס' 0010, 1.09.16)[60] – החוזר מסדיר את השימוש של מוסדות חינוך באמצעי קצה במסגרת תהליכי ההוראה, הלמידה וההערכה של תלמידים.

  חוזר המנכ"ל מתייחס באופן נרחב לשמירה על מידע ועל פרטיות ברמת השימוש היומיומי באמצעי הקצה. במובן זה, החוזר כולל מספר רב של המלצות למורים, הורים ותלמידים בנוגע לאופן השימוש שלהם באמצעי הקצה וביחס לאופן ההגנה על מידע על אודותיהם. כמו כן, החוזר מפנה לתקנים ולהנחיות טכנולוגיות שונים שהוצאו מטעם משרד החינוך לגורמים השונים המספקים את השירותים ואמצעי הקצה למוסדות החינוך, אשר בחלקם עוסקים בסוגיות של פרטיות ואבטחת מידע על אודות תלמידים.

- **חוזר מנכ"ל "מצלמות במוסדות החינוך – הסדרת הכנסתן ואופן התקנתן"** (הוראת קבע מס' 0119, 3.5.15)[61] – החוזר מסדיר את סוגיית השימוש של מוסדות חינוך במצלמות אבטחה/מעקב בתוך שטח בית הספר.

  חוזר המנכ"ל מדגיש את חשיבותה של הזכות לפרטיות עבור תלמידים ומסדיר את סוגיית השימוש במצלמות. החוזר מתייחס למכלול רחב של סוגיות הנוגעות לפרטיות תלמידים – משאלת עצם הצורך במצלמות, דרך סוגיית מיקום המצלמות ומחיקת המידע המוקלט, וכלה בהסדרת סוגית אבטחת המידע וזהות הגורמים הרשאים לצפות בו.

- **חוזר מנכ"ל "שמירה על פרטיות באתרי האינטרנט הבית-ספריים"** (תשס"ג/7 (א) 2.3.03)[62] – חוזר המסדיר את אופן ההתנהלות של גורמים חינוכיים שונים (מנהלים, מפקחים, מורים וגננות) בנוגע לשמירה על פרטיות תלמידים באינטרנט.

59 | ריכוז זה כולל את חוזרי המנכ"ל שפורסמו על-ידי משרד החינוך נכון למועד פרסום מדריך זה. יצוין כי על פי משרד החינוך, קיימים כיום מספר חוזרי מנכ"ל בנושא פרטיות תלמידים שטרם פורסמו, ושככל הנראה יפורסמו בעתיד.

60 | https://apps.education.gov.il/Mankal/Horaa.aspx?siduri=31.

61 | https://apps.education.gov.il/mankal/horaa.aspx?siduri=134.

62 | http://cms.education.gov.il/educationcms/applications/mankal/arc/sc7ak3_6_3.htm.

חוזר המנכ"ל מדגיש את חשיבות ההגנה על פרטיות תלמידים במסגרת השימוש של גורמים חינוכיים שונים (מנהלים, מפקחים, מורים וגננות) באינטרנט. במרכזו קובע החוזר מהו המידע הנוגע לתלמידים שמותר לגורמים חינוכיים לפרסם באתר האינטרנט של המוסד החינוכי, וזאת רק לאחר קבלת הסכמה בכתב של הורי התלמידים והתלמידים עצמם. כמו כן, החוזר קובע איסור מפורש לפרסם באתר הבית ספרי מידע מסוג כתובת התלמיד ומספר הטלפון שלו; מידע רגיש הנוגע לצנעת אישיותו, משפחתו ומצבו הכללי; מידע אודות ציונים והערכות לימודים, למעט מידע "מאובטח ומוגן" המאפשר גישה של התלמידים לציוניהם (מערכות משו"ב וכדומה). החוזר מציין כי בכל מקרה יש להקפיד שלא ייכללו באתר האינטרנט של המוסד החינוכי תכנים או תמונות "העלולים לבייש או להשפיל את באי המוסד החינוכי".

- **חוזר מנכ"ל "אתיקה ומוגנות ברשת האינטרנט"** (תשע"ב/4(א) 1.12.11)[63] – החוזר עוסק בנוהלי התקשורת הראויים בקרב מורים, תלמידים והורים במרחבי הרשת בדגש על תקשורת באתרים בית-ספריים, ברשתות חינוכיות וברשתות חברתיות.

חוזר המנכ"ל קובע כללים להגנה על פרטיות תלמידים במסגרת הקשר עם גורמי חינוך ברשת. כך, החוזר קובע כי "לא יפורסמו פרטים העלולים לפגוע בצנעת הפרט, בין אם של תלמיד, של איש סגל הוראה או של אדם אחר" וכי "תובטח אי-העברת מידע ופרטים אישיים לגופים חיצוניים". כמו כן, החוזר קובע כי "המוסד החינוכי יקפיד על הימנעות מפרסום מידע העלול לפגוע באנשי הצוות, בתלמידים, במשפחותיהם, בבית הספר וברגשות הציבור, ויסיר מידע כזה אם פורסם". החוזר קובע גם כי "איש צוות חינוכי לא יעשה שימוש במידע אישי/חברתי/משפחתי של התלמיד שנחשף אליו באקראי או בעקיפין, למעט במקרים שבהם מדובר במצבי סיכון בכפוף להנחיות בחוזרי המנכ"ל". בהתאם להוראות ה- COPPA (Children Online Privacy Protection Act) חוזר המנכ"ל קובע כי בתי ספר אינם רשאים ליזום או לעודד פעילות תלמידים מתחת לגיל 13 ברשתות חברתיות.

- **חוזר מנכ"ל "איחוד המקצועות למדעי הטכנולוגיה ומוט"ב למקצוע אחד – מדע וטכנולוגיה לכול"** (הוראת קבע מס' 0030, 13.10.16)[64] – החוזר עוסק בהסדרת מקצוע לימודי שמטרתו לחנך תלמידים לאוריינות מדעית-טכנולוגית וזאת, בין היתר, במטרה לחנכם לשמירה על פרטיות.

- **חוזר מנכ"ל "אקלים חינוכי מיטבי והתמודדות מוסדות חינוך עם אירועי אלימות וסיכון"** (הוראת קבע, 1.4.15)[65] – החוזר מסדיר את סמכויות ואופן התנהלות מוסדות חינוך עם אירועי אלימות וסיכון, לרבות אופן יישום חובות הדיווח בהתאם להוראות חוק העונשין, התשל"ז-1977.

63 | http://cms.education.gov.il/EducationCMS/Applications/Mankal/EtsMedorim/9/9-4/HoraotKeva/K-2012-4-1-9-4-10.htm

64 | https://apps.education.gov.il/mankal/horaa.aspx?siduri=13.

65 | https://apps.education.gov.il/mankal/horaa.aspx?siduri=132.

חוזר המנכ"ל קובע כי טיפול במקרי אלימות ייעשה, בין היתר, תוך שמירה על זכויותיהם של תלמידים, לרבות זכותם לפרטיות. חוזר המנכ"ל קובע את הדברים הן באופן עקרוני והן תוך התייחסות נקודתית לאופי המקרים השונים. חוזר המנכ"ל מתייחס בהקשר זה, בעיקר, להגנה על פרטיות "פיזית" של תלמידים, ולא לסוגיות של פרטיות במידע. חריג בהקשר זה הוא התייחסות החוזר לאופן התנהלות מוסדות חינוך בכל הנוגע לחיפוש בטלפונים ניידים של תלמידים. כך לדוגמה, החוזר קובע כי "אין לערוך חיפוש במכשיר הפרטי של התלמיד. המידע יוצג על ידי התלמיד והוריו. במקרה של פרסום תצלום, סרט או הקלטה של אדם המתמקד במיניותו, יש לערוך את הבירור בנפרד. אם יש כמה נפגעים יש לפגוש כל אחד מהם לחוד. אם הוגשה תלונה יש לפעול בהתאם להנחיות המשטרה". בנוסף, החוזר קובע מגבלות בנוגע לפרסום מידע על אירועי אלימות תוך שהוא מציין, בין היתר, כי חל איסור על מסירת פרטים שעלולים לזהות את הילדים המעורבים.

חוזר המנכ"ל מתייחס באופן מינורי להיבטים של איסוף ושמירת מידע. כך, סעיף 3.9.3, הדן באפשרות להשעיה דחופה של עובד הוראה על-ידי מנכ"ל המשרד בשל חשד לעבירה חמורה בתלמיד, קובע כי דיווחים בעניינים אלו יישמרו במאגר מידע שינוהל על-ידי גורם במשרד. החוזר מבהיר כי מאגר המידע לא יכלול את שמות הילדים הנפגעים.

- **חוזר מנכ"ל "ראמ"ה – מערך המבחנים, המחקרים והסקרים הארציים לשנת הלימודים התש"ף** (הודעה מס' 0172, 5.11.19)[66] – חוזר המנכ"ל מתייחס להנחיות ראמ"ה (רשות ארצית למדידה והערכה בחינוך), בנוגע לעריכת סקרי הערכה בבתי ספר בשנת הלימודים תש"ף (הודעות דומות הוצאו גם בשנים קודמות). חוזר המנכ"ל מציין בקצרה כי "בעת ביצוע הסקר תהיה בכיתות הקפדה מלאה על פרטיות התלמידים", וכי על המורה המעביר את הסקר "לכבד את פרטיות המידע הנרשם על ידי התלמידים".
- **חוזר מנכ"ל "נהלים לפעילות מחקרית במערכת החינוך"** (הוראת קבע מס' 0123, 3.5.2015)[67] – חוזר המנכ"ל מסדיר את הפעילות המחקרית המתקיימת במערכת החינוך. חוזר המנכ"ל מסדיר את הפעילות המחקרית המתקיימת במערכת החינוך. החוזר מתייחס לסוגיה של הגנת פרטיות תלמידים במסגרת הליך המחקר עצמו. כך, סעיף 1.5.10 לחוזר קובע כי על עורך המחקר ועל הנהלת המסגרת החינוכית להבטיח כי במהלך איסוף המידע יישמרו כלל זכויותיהם של הנבדקים, לרבות זכותם לפרטיות. הסעיף מבהיר ש"אם הנבדקים הם תלמידים, תישמר פרטיותם ככל האפשר, בלי לפגוע בחובת ההשגחה של צוות המסגרת החינוכית עליהם".

66 | https://apps.education.gov.il/mankal/hodaa.aspx?siduri=159.

67 | https://apps.education.gov.il/mankal/horaa.aspx?siduri=129.

החוזר מתייחס לסוגיות של איסוף מידע, ובמסגרת זו קובע כללים המסייגים את איסופו של מידע המאפשר זיהוי של הגורם הנחקר. כך לדוגמה, סעיף 1.5.11 קובע כי "ככלל לא יותרו איסוף מידע או שמירה של מידע שנאסף באופן המאפשר את זיהוים של הנבדקים על ידי גורם כלשהו, ובכלל זה עורך המחקר עצמו". בהמשך קובע החוזר כי במידה ויותר איסוף מידע מזהה, איסוף זה יותנה בקבלת הסכמה בכתב של הנבדק, כנדרש על פי הוראות חוק הגנת הפרטיות. החוזר מציין כי במידה ומדובר בתלמיד – יש לקבל את הסכמתו לכך והסכמה מדעת של הוריו (אשר צריכה להתקבל בכתב). סעיף 1.5.12 לחוזר אוסר, ברמה העקרונית, פרסום מידע הניתן לזיהוי.

- **חוזר מנכ"ל "האיסור לאפשר איסוף מידע במוסדות החינוך ו/או באמצעותם ע"י גופים חיצוניים ללא היתר לשכת המדען הראשי"** (תש"ע/3 .1.11.09)[68] – החוזר קובע כי אין לאפשר לגורם כלשהו שאינו פועל מטעם המשרד להיכנס למוסד חינוך לצורך איסוף מידע, אלא באישור לשכת המדען הראשי.

- **חוזר מנכ"ל "מביקור סדיר למניעת נשירה"** (הוראת קבע מס' 0013, 1.3.17)[69] – חוזר המנכ"ל מסדיר את פעילות מערך הביקור הסדיר במערכת החינוך. החוזר מפרט את ההנחיות, ההליכים והפעולות שעל הרשויות המוסמכות (ובעלי התפקידים השונים) במערכת החינוך לנקוט לצורך קיום ומימוש הוראות חוק לימוד חובה.

  החוזר מתייחס, בין היתר, גם להיבטים של שימוש במידע. כך, סעיף 3.3.3 מגדיר את מאגר המידע של הרשות, אשר אוגר מידע אישי של תלמידים בגיל לימוד חובה. סעיף 3.4.2 מחייב את הרשות להקצות משאבים לקיומה והפעלתה של מערכת מידע ממוחשבת, שנועדה "לאפשר לקצין הביקור הסדיר לתעד את עבודתו עם התלמידים החייבים ברישום ובביקור במוסד חינוך מוכר ולנהל מעקב אחריהם". סעיף 5.4.7 קובע כי: "לצורך ביצוע הפעולות האמורות לעיל ינהל קצין הביקור הסדיר תיק לכל תלמיד שבטיפולו במערכת המידע הממוחשבת של משרד החינוך, ויכלול בו תיעוד של הליכי הטיפול ושל ההמלצות/ ההחלטות בעניינו של התלמיד".

- **חוזר מנכ"ל "חינוך מיוחד יישום חוק החינוך המיוחד: ועדת שילוב מוסדית, ועדת השמה ביושבה כערר על ועדת שילוב, ועדת השמה וועדת ערר"** (הוראת קבע מס' 0201, 20.2.19)[70] – חוזר המנכ"ל מסדיר את ההליך הפרוצדוראלי של הפניית תלמידים לוועדות שונות הפועלות מכוח חוק חינוך מיוחד. תחת זאת, החוזר מסדיר מספר היבטים הנוגעים לפרטיות תלמידים, לרבות הגנה ושמירה על מידע הנוגע אליהם. חוזר המנכ"ל קובע, בין היתר, כי שמירת המסמכים שהובאו לפני ועדת ההשמה או ועדת ערר תיעשה על פי התקנות להגנת הפרטיות (תנאי

68 | http://cms.education.gov.il/EducationCMS/Applications/Mankal/EtsMedorim/3/3-9/HodaotVmeyda/H-2010-3-3-9-1.htm

69 | https://apps.education.gov.il/mankal/horaa.aspx?siduri=37.

70 | https://apps.education.gov.il/mankal/horaa.aspx?siduri=235

החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986. בנוסף, ס' 2.13, העוסק בניהול הנתונים של ועדות השמה באמצעות מערכת אינטרנטית, קובע כי "יש להקפיד שבתהליך העברת המידע הנוגע לתלמיד יושם דגש על סודיות המידע תוך שמירה על צנעת הפרט".

- **חוזר מנכ"ל "התכנית הלאומית ללמידה משמעותית – מבחנים פנימיים כחלק מהערכה על פני הרצף החינוכי"** (הוראת קבע מס' 0073, 8.5.16)[71] – החוזר מתווה דרכים לשימוש מוסדות החינוך במבחנים פנימיים כחלק ממתכונת הערכה של תלמידים. החוזר קובע, בסעיף 3.5, כי המידע על תפקוד הילד בגן יועבר להוריו במפגשים פרטניים וכי העברת מידע לכל גורם אחר תהיה "בכפיפות לחוק הגנת הפרטיות, התשמ"א-1981, ולחוק חופש המידע, התשנ"ח-1998, ועל פי כללי האתיקה המחייבים".
- **חוזר מנכ"ל "מעבר בתי הספר היסודיים לניהול עצמי: עקרונות המדיניות ומודל היישום"** (הוראת קבע מס' 0041, 1.10.17)[72] – חוזר המנכ"ל מסדיר את עקרונות המעבר של בתי ספר יסודיים לפעילות בניהול עצמי. חוזר המנכ"ל לא דן במערכת היחסים בין המוסד החינוכי לתלמידיו ומכאן שהוא לא כולל כל התייחסות ישירה לסוגיות של פרטיות. עם זאת, סעיף 15 לחוזר מסדיר את סוגיית גיבוי ואבטחת המידע הדיגיטלי בבית הספר.

  כך לדוגמה, החוזר קובע שאין לאפשר לגורמים שלא הוסמכו על ידי הרשות המקומית ו/או על ידי מנהל בית הספר וכן לכל מי שאין לו נגיעה למערכת הכספית של בית הספר, לעיין בדוחות/בתיקים/במסמכים. החוזר מחייב את בתי הספר בביצוע גיבויים למידע וקובע כי "על בית הספר לעמוד בכל הסטנדרטים של אבטחת המידע", תוך שהוא מציין כי האחריות בעניין זה מוטלת על הרשות המקומית בה פועל בית הספר. כמו כן, החוזר קובע כי "הרשות ומשרד החינוך יוודאו רישום מערכות מידע על פי חוק מאגרי המידע".
- **חוזר מנכ"ל "מעברים – רצף חינוכי מהגן לבית הספר"** (הוראת קבע מס' 0156, 6.1.19)[73] – החוזר עוסק במעבר תלמידים משלב חינוכי אחד למשנהו. חוזר המנכ"ל קובע, בין היתר, כי העברת מידע חינוכי-טיפולי מצוות הגן לצוות בית הספר תיעשה, עם המעבר של הילד, רק בהסכמת ההורים ובעקבות חתימתם על טופס ויתור סודיות. עיקרון זה חל גם ביחס לכל מעבר של תלמיד משלב חינוכי אחד למשנהו ו/או בין מוסד חינוכי אחד לאחר.
- **חוזר מנכ"ל "ביעור רשומות בבתי הספר"** (תשס"א/8(א), 1.4.00)[74] – חוזר המנכ"ל מגדיר את סוגי המסמכים הנדרשים לשמירה על-ידי משרד החינוך והרשויות המקומיות, תוך הסדרת

71 | https://apps.education.gov.il/mankal/horaa.aspx?siduri=235.

72 | https://apps.education.gov.il/mankal/horaa.aspx?siduri=47.

73 | https://apps.education.gov.il/Mankal/Horaa.aspx?siduri=216.

74 | http://cms.education.gov.il/EducationCMS/applications/mankal/arc/sa8ak3_7_18.htm.

סוגיית ביעור החומרים הרלוונטיים ומועדי השמירה הנדרשים לכל סוג מסמך. חוזר המנכ"ל אינו מתייחס ישירות לסוגיות של פרטיות ו/או הגנת מידע.

- **חוזר מנכ"ל "תקינה לתוכנה כספית לבתי ספר"** (הוראת קבע מס' 0164, 27.8.13)[75] – חוזר המנכ"ל מפרט את דרישות התקינה לתוכנה כספית התומכת את תפעול המערך הכספי בבתי הספר. לפי חוזר זה על המערכת לעמוד בהוראות הדין, לרבות חוק הגנת הפרטיות ותקנות להגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים).
- **חוזר מנכ"ל "מאגרי מידע בבתי ספר – רישום, דיווח ואבטחת מידע"** (תש"ע/3(א), 1.11.09)[76] – חוזר המנכ"ל מסדיר את סוגיית השימוש של בתי ספר במאגרי מידע והדיווח עליהם. החוזר קובע מספר הנחיות מרכזיות:

- החוזר מבהיר כי מאגרי המידע ה"ציבוריים" שבשימוש בתי ספר (מאגר מנב"ס) ומאגרי המידע המקומיים והפנימיים שנוצרים על-ידי בתי ספר לשימושם העצמי ו"לסיוע במעקב אחר תלמידים ובטיפול בהם" (כגון מאגרי מידע המכילים רשימות תלמידים שננקטו לגביהם פעולות חינוכיות, רשימות תלמידים בעלי בעיות אישיות, משפחתיות או כלכליות שונות), חייבים ברישום בפנקס מאגרי המידע.
- ברמה העקרונית החוזר מדגיש כי על בית הספר להקפיד להחזיק אך ורק במאגרי מידע הדרושים לו לצורך עבודתו הסדירה וקיום תפקידיו, וכי השימוש בנתונים המצויים במאגרי המידע מותר אך ורק לצורך המטרה שלשמה הוקם המאגר. החוזר מדגיש גם כי שימוש שלא כדין במידע או שימוש במאגרי מידע שלא נרשמו כדין אסור על פי החוק, ועלול אף להיחשב עברה פלילית.
- בכל הנוגע לרישום המאגרים, החוזר מבחין בין בתי ספר רשמיים לכאלו השייכים לחינוך המוכר שאינו רשמי ומוסדות הפטור. בכל הנוגע למוסדות רשמיים – החוזר מבהיר כי חובת הרישום של המאגרים (מאגר מנב"ס והמאגרים הפנימיים) חלה על משרד החינוך. מנגד, ביחס למוסדות המוכש"ר והפטור – החוזר קובע כי חובת הרישום חלה על הבעלויות של המוסדות.
- החוזר מחייב את מנהלי בתי הספר להעביר אליו דיווח שנתי ביחס למאגרי המידע הנמצאים תחת שימושם. חובה זו חלה גם ביחס למנהלים של מוסדות חינוך של המוכש"ר ומוסדות הפטור.

מעבר להנחיות אלו החוזר קובע כללים מפורטים בנוגע לשמירת ואבטחת מידע, הן ברמה הפיזית והן ברמה הטכנולוגית. החוזר מחייב את מנהל בית הספר במינוי ממונה על אבטחת

75 | https://apps.education.gov.il/mankal/horaa.aspx?siduri=152

76 | http://cms.education.gov.il/EducationCMS/Applications/Mankal/EtsMedorim/3/3-6/HoraotKeva/

מידע וכן קובע כללים רבים בנוגע ליישום ההגנה על מידע בית ספרי. כך לדוגמה, החוזר מזכיר את האפשרות של הורים לעיין במידע על אודות ילדם.

- **"הנחיות להעברת שיעור המתקיים בכיתה לתלמידים הלומדים מרחוק בתקופה הקורונה (למידה משולבת)" (נובמבר 2020)**[77] – ההנחיות מנחות מורים בנושא צילום והקלטה של שיעורים המתקיימים במסגרת של למידה משולבת. ההנחיות קובעות, בין היתר, כי השימוש במצלמות במסגרת זו כפוף להסכמת המורה, שאין לצלם את התלמידים הלומדים בכיתה, ושהצילום נועד הוא אך ורק לשם העברת שיעורים לתלמידים הלומדים מרחוק ולא למטרות אחרות.
- **הנחיות בנושא "מפגש כיתה וירטואלי"**[78] – סדרת מסמכים הכוללות פירוט בדבר "אקלים כיתה בטוח ותומך במרחב המקוון", וכן התייחסות ליישומים המשמשים ללמידה סינכרונית. התייחסות זו כוללת גם פירוט של הנחיות אבטחת מידע ביישומים הספציפיים הקיימים במערכת החינוך.
- **"הנחיות אבטחת מידע במוסדות חינוך" (יוני, 2019)**[79] – ההנחיות מנחות את מנהל בית הספר בעניינים שונים הנוגעים לאבטחת מידע במוסד החינוך. ההנחיות קבועות, לדוגמה, כי יש לוודא כי הרשאות הגישה למידע או השימוש במערכות יינתנו בהתאם לצורך של המשתמש לשימוש במידע. כמו כן, ההנחיות קובעות כי על מוסד החינוך לעשות שימוש אך ורק במוצרים חינוכיים טכנולוגיים אותם מספק משרד החינוך ובמוצרים שקיבלו אישור של משרד החינוך. ההנחיות מנחות את מנהל המוסד בעניינים הנוגעים לניהול והגנת מחשבי בית הספר כמו גם ביחס להגנות רשת. ההנחיות מתייחסות לסוגיה של שימוש בטוח בדואר אלקטרוני תוך שהיא קובעת כי "לצרכים פדגוגיים ומנהלתיים של בית הספר יש לעשות שימוש אך ורק בדוא"ל ארגוני מאובטח ולא בחשבונות דוא"ל פרטיים". כמו כן ההנחיות מתייחסות, בין היתר, לסוגיית גיבויי המידע וכן מפרטות את אופן ההתנהלות הנדרש במקרים של "אירועי אבטחת מידע".
- **"מדיניות שמירה וטיפול במידע מוגן"**[80] – המסמך מגדיר את אופן התנהלותם של בתי ספר בכל הנוגע לשמירה, העברה והצגה של מידע "מוגן". המסמך מגדיר היכן מותר לבתי ספר לשמור מידע מוגן, (בהקשר זה הוא קובע כי שמירה שכזו אפשרית גם סביבת ענן בית ספרית), תוך שהוא מבהיר כי שמירת מידע במחשבים פרטיים, התקנים ניידים, מחשבי בית ספר ציבוריים וחשבונות ענן פרטיים – היא אסורה. המסמך מציין כי יש להקפיד כי במקומות בהם נעשה

77 | https://poh.education.gov.il/PniotVemokdeiSherut/Pages/hybrid-class.aspx

78 | https://pop.education.gov.il/sherutey-tiksuv-bachinuch/virtual-classroom-meeting/

79 | https://sites.education.gov.il/cloud/home/tikshuv/Documents/hanchayot_havtachat_mida_batisefer.pdf.

80 | https://sites.education.gov.il/cloud/home/havtachat_mida/Documents/mediniyut_shmira_vetipul_bemeyda_mugan_bemosadot.pdf

שימוש לשמירת מידע מוגן, הגישה למידע תבוצע באמצעות הרשאות גישה שונות לאנשי הצוות. בכל הנוגע להעברת מידע – המסמך קובע כי אין לעשות שימוש בחשבונות פרטיים כגון דוא"ל פרטי ותוכנות מסרים. לפי המסמך, העברת מידע צריכה להתבצע רק באמצעות האמצעים אותם מעמיד בית הספר לשימוש כגון דוא"ל בית ספרי ושירותי ענן בית ספריים.

- **"תקן תנאי שימוש/פרטיות למוצרים טכנולוגיים בחינוך"** (4.9.14)[81] – מסמך זה מגדיר תקן והנחיות לתנאי שימוש במוצרים טכנולוגיים חינוכיים המפורסמים על ידי הספקים והגופים המפתחים. להלן שתי ההנחיות המרכזיות הקבועות במסמך אשר רלוונטיות לסוגיית הגנה על פרטיות תלמידים:
  - סע' 1.2 למסמך קובע כי איסוף המידע במערכת ייעשה בהתאם להוראות הדין (לרבות חוק הגנת הפרטיות והתקנות שנתקנו על פיו), ובהתאם לאישור פרטני, רשמי ובכתב מטעם משרד החינוך. המסמך מדגיש כי אין לאסוף מידע על אודות תלמידים.
  - סע' 1.3 למסמך קובע כי לגורמים המפעילים את המערכות אסור להעביר את המידע הנאסף במסגרת המערכת הטכנולוגית לצדדים שלישיים או לכל גורם אחר, לרבות חברות המספקות שירותי תמיכה. כמו כן, אין לעשות שימוש במידע אלא אם התקבל אישור פרטני מטעם משרד החינוך.
- **"תקנים והנחיות טכנולוגיות כלליות עבור ספקים וגופים מפתחים"**[82] – בנוסף להנחיות שפורטו עד כה משרד החינוך קובע גם תקנים והנחיות טכנולוגיות כלליות עבור ספקים וגופים מפתחים.

על פי הנחיות אלו, על כל ספק חדש המבקש לקבל נתוני תלמידים לעבור תהליך אישור ו"התקנת כספת" על מנת להיות ספק מורשה במשרד החינוך. לפי תרשים הליך קבלת האישור, השלבים לקבלת האישור כוללים, בין היתר, בדיקה טכנולוגית ובדיקות אבטחת מידע.

- **"תקן אבטחת מידע"** (גרסה 2.5, 4.12.16)[83] – מסמך זה כולל אוסף מפורט של דרישות אבטחת מידע לספקי מוצרים חינוכיים טכנולוגיים, אשר לפי המסמך, עמידה בהן מהווה תנאי סף לקבלת אישור מטעם משרד החינוך לפעול במסגרתו.

המסמך קובע כי המידע המצוי במאגרי המידע של המשרד ו/או נאסף או נוצר במסגרת פעילות של המשרד או מוסדות חינוך אשר בידי הספק או שיש לספק גישה אליהם, הוא

81 | https://sites.education.gov.il/cloud/home/meyda_le_sapakim/Documents/teken_tnaey_shimush_pratiut.pdf.

82 | לעיון בתרשים הליך קבלת האישור לספק/ית חדש/ה, ראו: https://sites.education.gov.il/cloud/home/meyda_le_sapakim/Documents/madrich_sapak_hadash.pdf

83 | https://sites.education.gov.il/cloud/home/meyda_le_sapakim/Documents/teken_avtahat_meyda.pdf. המסמך מהווה תקן סופי מתאריך 1.12.13.

בבעלות משרד. לפי המסמך, הספק מתחייב שכל גישה שלו, או של מי מטעמו, למידע ולמאגר המידע, תתבצע אך ורק בהתאם להוראות המשרד ולמטרות אשר הוגדרו לו על ידי המשרד. כמו כן, הספק מתחייב שהוא, או מי מטעמו, יקפיד כי כל איסוף מידע או שימוש בו יבוצע אך ורק בהתאם להוראות החוק והדין ועל פי הנחיות המשרד, וכן שהוא, או מי מטעמו, לא יעביר מידע, או חלק ממידע, מתוך מאגרי המשרד אשר בידיו או שיש לו גישה אליהם, לצד שלישי כלשהו ללא אישור מפורש ובכתב מאת המשרד.

סעיף 3.7.4 למסמך מסדיר את השימוש של ספקים במאגרי מידע מחוץ לגבולות ישראל. המסמך קובע כי הוצאת מידע לשרתים שכאלו תתאפשר, בין היתר, תוך כדי נקיטת אמצעים שלא יפחתו מהמפורט בתקנות הגנת הפרטיות (העברת מידע אל מאגרי מידע שמחוץ לגבולות המדינה), התשס"א-2001. המסמך קובע כי העברת המידע תתאפשר רק למדינות החברות באיחוד האירופי וכן שניתן לאחסן שירותים בשירותי ענן שאינם ממוקמים בישראל, אך לא כאלה המאחסנים מידע מוגן/חסוי. כמו כן המסמך קובע את העיקרון לפיו הוצאת מידע מהמערכת תעשה רק בהתאם לרלוונטיות שלו.

המסמך מחייב את הספקים בביצוע ניהול וזיהוי של סיכוני אבטחת מידע לפי הצורך וקובע כללים שונים בנוגע לאבטחת מידע (דיגיטלית ופיזית), תוך הבחנה בין סוגי המידע (בלמ"ס, מוגן או חסוי). כמו כן, המסמך מחייב את הספק לפעול בהתאם להוראותיו בכל הנוגע לניהול הרשאות הגישה למידע.

בכל הנוגע לניהול המידע סעיף 3.18.4 למסמך קובע מפורשות כי הספק מתחייב שלא להעביר מידע מוגן או חסוי הנמצא בבעלות משרד החינוך לגורם שלישי ללא אישור בעל המידע במשרד החינוך.

סעיף 6 למסמך מתייחס לסוגיית הגנת המידע באפליקציות "מובייל" (נייד). כך, בין היתר, המסמך קובע בעניין זה כי "האפליקציה לא תשמור מידע מוגן או חסוי במכשיר ללא הצפנת הנתונים". סעיף 6.1.2 קובע כי "האפליקציה תאפשר למשתמשים למחוק את כל הנתונים הקשורים אליה באופן פשוט וברור". סעיף 6.3.2 מרחיב את נקודת המבט וקובע כי "בכל שימוש בחיישנים או ברכיבים נוספים הקשורים למכשיר יש ליידע ולבקש את אישור המשתמש""

- **"הנחיות והמלצות לסביבות ענן לחינוך"**[84] – הנחיות אלו מנחות מוסדות חינוך לשמירה על פרטיות ואבטחת מידע ביישומי ענן הפועלים במערכת החינוך (מטעם חברת Google ו-Microsoft). הנחיות אלו קובעות כי מנהל מוסד החינוך הוא הגורם האחראי לקיום הנחיות אבטחת המידע בבית הספר בסביבת יישומי ענן. ההנחיות מחייבות מינוי מנהל סביבה וכן

84 | https://sites.education.gov.il/cloud/home/svivot_anan_hinuch/Pages/havtacha.aspx.

קובעות כללים בנוגע לזיהוי מנהל זה. ההנחיות קבועות גם כי "יש לאפשר למשרד החינוך גישה לסביבת הענן לצרכי בקרה, תחקור וטיפול באירועי אבטחת מידע, במידה ויתרחשו".

סעיף 10 להנחיות קובע כי ככלל, יש לשים לב לסיווג המידע אותו ניתן להעביר ולשמור לסביבות הענן המאושרות. ההנחיות קובעות שבמידה והאישור שניתן הוא למידע שאינו מוגן, חל איסור להעביר או לשמור מידע רגיש או חסוי אודות פרטי התלמידים, הוריהם ואנשי הצוות החינוכי לרבות: מספרי ת"ז, תאריכי לידה, כתובת, טלפונים, שמות הורים, ציונים וכו'.

ההנחיות קובעות גם כי על מנהל היישום (אדמיניסטרטור) לוודא כי לא ניתן יהיה לשמור, לנהל ולקבל עדכון על מיקום הפיזי של הטלפון הנייד השייך למשתמשים באמצעות יישום הענן, וכי מידע לא יסונכרן באופן אוטומטי בין המכשיר הנייד של משתמשים ליישום הענן המנוהל על ידי המוסד חינוכי. ההנחיות קבועות מגבלה בנוגע לקשר בין יישומי הענן לתוכנות הפועלות מחוצה לו, תוך שהן קובעות שילדים על גיל 13 יפעלו בסביבה חסומה, בעוד ילדים מעל גיל זה יהיו בסביבה פתוחה, בכפוף לאישור הוריהם.

בנוסף להנחיות האמורות, משרד החינוך מפרסם גם הנחיות אבטחת מידע ספציפיות לשימוש מוסדות חינוך בסביבות הענן של חברות Google ו-Microsoft. כך לדוגמה, ביחס לסביבת הענן של Google, נכתב כי במסגרת הבקרה על השירות, יש לבחון דוחות אבטחת המידע מסוימים (התחברות ממקורות לא ידועים, התחברות סימולטנית ממספר גיאוגרפיות, שינויים בהגדרות הניהוליות של המערכת), ולבצע בדיקה אחת לשבוע "על מנת לאתר שימוש לא תקין במערכת". ההנחיות מורות על שימוש במערכת למניעת זליגת מידע (DPL) רגיש, כגון "נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמנותו, ופרטים מזהים כגון: תעודת זהות ותמונה". בכל הנוגע לעבודה עם דפדפן chrome, ההנחיות קובעות כי יש לחסום את האפשרות למעקב אחר מיקום גיאוגרפי של המשתמשים בדפדפן.

עד כאן פירוט המסמכים המרכזיים העוסקים באבטחת מידע. יצוין כי ישנם מסמכים נוספים המסדירים עניינים טכנולוגיים כאלו ואחרים הקשורים באופן מינורי יחסית לסוגית פרטיות מידע על אודות תלמידים, כגון "תקן טכנולוגי למערכות ניהול למידה (LMS) מיום 28.6.15, "תקן לספרים דיגיטליים – רמה מתקדמת" מיום 8.3.16.

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

073-3928555 | PPA@justice.gov.il | WWW.GO.GOV.IL/PPA

קרית הממשלה, ת.ד. 7360, תל אביב 6107202 | חפשו אותנו גם בפייסבוק