20 אוגוסט 2020
ל' באב תש"פ

הגנת פרטיות תלמידים בלמידה מרחוק: דגשים והמלצות להתנהלות בתקופת התמודדות עם נגיף הקורונה

מסמך מעודכן לקראת פתיחת שנת הלימודים תשפ"א[1]

רקע

הניסיון למנוע ולצמצם את התפשטות נגיף הקורונה בישראל וההנחיות למניעת התקהלויות מרובות משתתפים יצרו מציאות חדשה בה תלמידים (מכלל הגילאים ושלבי החינוך) נדרשים להעביר חלק ניכר מזירת הפעילות הלימודית שלהם מספסלי הלימודים לביתם הפרטי. אם בתחילת המשבר המחשבה הייתה שהוא יחלוף תוך מספר חודשים, ההבנה כיום היא שאנו צפויים לחיות ב"שגרת קורונה" לתקופה ממושכת. לפיכך, עם פתיחת שנת הלימודים יתחילו עשרות אלפי תלמידים לקיים תהליכי למידה מרחוק באמצעות יישומים דיגיטליים מקוונים (יישומי e-learning; edTech).

תהליך זה יתקיים במסגרת **פלטפורמות ללמידה מרחוק** ובמסגרת שימוש תלמידים **בסביבות תוכן מתוקשבות**. למידה מרחוק (או למידה מקוונת) היא מסגרת של העברת שיעורים באופן מקוון, על-פי רוב בזמן אמת ובשידור "חי" לתלמידים, שעה שאלו נמצאים מחוץ לכותלי מוסדות החינוך. במסגרת זו עשויים מוסדות חינוך לעשות שימוש ביישומים מסחריים שונים, כגון Microsoft Teams, Zoom או Skype. סביבות תוכן מתוקשבות הן 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, כאשר לכל תלמיד ניתן קוד אישי בעזרתו הוא יכול "להיכנס" לסביבה ולפעול במסגרתה. דוגמאות לתוכנות אלו הן 'אופק' - סביבה דיגיטלית אינטראקטיבית ללמידה של מטח (המרכז לטכנולוגיה חינוכית), ותוכנת 'עשר אצבעות' של חברת matific. במסגרת מסמך זה נתייחס לכלל היישומים שפורטו לעיל כיישומים דיגיטליים ללמידה מרחוק.

ככלל, יש יתרונות רבים במודל הלמידה מרחוק. עם זאת, המודל מהווה אתגר מבחינת ההגנה על פרטיות תלמידים. בנסיבות הקיימות, המעבר למודל כזה או אחר של למידה מרחוק הוא מתבקש אך יש להקפיד כי יישום תהליכי הלמידה במסגרת מודל זה יהלום את עקרונות הגנת הפרטיות.

השימוש הנרחב של מוסדות חינוך ביישומים ללמידה מרחוק עשוי להשליך על פרטיותם של תלמידים רבים, לרבות בהיבטים של ההגנה על מידע אישי הנוגע אליהם. יישומים דיגיטליים

[1] מסמך מעודכן זה נכתב לקראת פתיחת שנת הלימודים תשפ"א במוסדות חינוך והוא עוסק בפרטיות תלמידים הלומדים בגנים, בתי ספר יסודיים, חטיבות ביניים וחטיבות עליונות. מסמך בתחום ההשכלה הגבוהה יפורסם באופן נפרד בהמשך.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

ללמידה מרחוק הם ברובם יישומים האוספים מידע על משתמשים, לרבות מידע רגיש, כגון נתונים הנוגעים לזהות התלמידים ונתונים בדבר ההישגים הלימודיים שלהם. שימוש ביישומים האמורים עשוי להביא גם לאיסוף מידע הנוגע לתלמידים שאינו נובע ישירות מהתהליך הלימודי, כגון מידע על אודות הרגלי הגלישה של התלמידים וכתובות מגוריהם. על-פי רוב, מידע זה נאסף ונשמר במאגרי מידע של החברות שהיישומים נמצאים בבעלותם ותחת ניהולם. כמו כן, מידע זה עשוי להיות מעובר לגורמים שונים. כך לדוגמה, על פי פרסומים באמצעי התקשורת, בארץ ובעולם הוגשו תובענות ייצוגיות כנגד מפעילי פלטפורמות שונות, בטענה שהעבירו לכאורה מידע על אודות משתמשים בשירותיה לצדדים שלישיים מבלי ליידע את המשתמשים על כך.[2]

ככלל, 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 אודות תלמידים עשוי להיחשף, לדלוף ולהגיע לידי גורמים שמידע זה אינו אמור להיות בחזקתם. כך לדוגמה, בחודשים אפריל-מאי 2020 דיווחה חברת צ'ק פוינט על מציאת חולשות אבטחת מידע ביישומים שונים ללמידה מרחוק,[3] לרבות במערכת 'אופק' בה משתמשים מוסדות חינוך ישראלים רבים.[4]

חשיפת מידע על אודות תלמידים עשויה להיגרם גם כתוצאה מפעילות גורמים אחרים המקיימים אינטראקציות עם תלמידים על גבי היישומים האמורים, כגון תלמידים אחרים ומורים. אחד החששות הבולטים של תלמידים בהקשר זה הוא צילומם בעודם משתתפים בשיעורים, ופרסום התמונות ברבים. בפרויקט מיוחד של מנהיגות נוער לפרטיות שמפעילה הרשות להגנת הפרטיות בשיתוף משרד החינוך הכולל מפגשי הדרכה ולמידה, הועלתה מצד התלמידים תהייה ביחס לחיובם "לפתוח" מצלמות במסגרת שיעורים מקוונים. חלק מהתלמידים ציינו שחשיפת המרחב הפרטי שלהם ברשת פוגעת בפרטיותם, וכן שהם חוששים שתלמידים אחרים יצלמו אותם ויפיצו את תמונתם ברשתות חברתיות, באופן שעשוי להשפילם. שאלות דומות הועלו גם ביחס לחיוב השימוש במצלמות בזמן בחינות.

עוד יש לזכור כי 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, שאיסוף מידע מהווה רכיב מרכזי בפעילותם. יש לזכור כי ככלל, ילדים מודעים פחות לניסיונות "לדוג" מידע הנוגע

---

[2] עודד ירון "בקשה לתביעה ייצוגית נגד זום בטענה לפגיעה בפרטיות ושיתוף מידע עם פייסבוק" **הארץ** (12.4.20), https://www.haaretz.co.il/captain/software/.premium-1.8761124; Isobel Asher Hemilton, *Zoom is being sued for allegedly handing over data to Facebook*, BUSINESS INSIDER (Mar. 31, 20), https://www.businessinsider.com/zoom-sued-allegedly-sharing-data-with-facebook-2020-3.

[3] הגר בוחבוט "חולשות אבטחה במערכות למידה מרחוק" **ynet** (30.4.20), https://www.ynet.co.il/digital/technews/article/SkSK4luFL.

[4] יסמין יבלונקו "הורים לתלמידים? שימו לב: חולשות אבטחה חמורות התגלו במערכת הלמידה מרחוק "אופק" **גלובס** (4.5.20), https://www.globes.co.il/news/article.aspx?did=1001327296.

אליהם, וכן נוהגים לא פעם לחשוף ברשת מידע על אודותיהם או על בני משפחתם, באופן העשוי לפגוע בהם ובעתידם.

פתיחת שנת הלימודים תיעשה השנה בצל התמודדות מערכת החינוך עם נגיף הקורונה ומעבר מוסדות חינוך רבים למודל של למידה מרחוק. לאור האמור, מטרת המסמך היא להציג מספר דגשים והמלצות להתנהלות נכונה ולהגנה על פרטיות ומידע אישי במסגרת שימוש תלמידים ביישומי למידה מרחוק. מסמך זה נועד בחלקו הראשון עבור תלמידים והוריהם. חלקיו השני והשלישי של המסמך מיועדים לגורמים המנהלים תהליכי למידה מרחוק מטעמם עבור ילדים (כגון מוסדות חינוך, רשויות מקומיות וגורמים פרטיים כגון תנועת הצופים ודומיה), אשר מתקשרים עם גורמים חיצוניים להפעלת יישומים דיגיטליים ללמידה מרחוק. **יודגש כי מסמך זה אינו עוסק בתחום ההשכלה הגבוהה אלא בפרטיות תלמידים במוסדות חינוך (חינוך קדם-יסודי, חינוך יסודי, חטיבות ביניים וחטיבת עליונות). מסמך בתחום ההשכלה הגבוהה יפורסם בהמשך.**

<u>דגשים והמלצות להתנהלות נכונה מצד משתמשים (הורים ותלמידים)</u>

למשתמשים ביישומים הדיגיטליים ללמידה מרחוק, כגון תלמידים (והוריהם) יש תפקיד משמעותי בצמצום ומזעור האפשרות לפגיעה בפרטיותם, ובפרטיות אחרים. להלן מספר כללים פשוטים ליישום העשויים להביא לחיזוק ההגנה על הפרטיות במסגרת שימוש ביישומים ללמידה מרחוק:

- השתמשו בסיסמאות חזקות למחשב וליישומי הלמידה מרחוק בהם אתם משתמשים. הקפידו להחליף את הסיסמה המקורית שקיבלתם לשימוש ביישום והחליפו אותה בסיסמה בת לפחות 8 תווים, הכוללת אותיות (מומלץ בשילוב אותיות בשפות שונות, או גדלים שונים – אותיות קטנות וגדולות), מספרים, ותווים מיוחדים. זכרו להשתמש בסיסמאות שונות לשירותים שונים. כמו כן, מומלץ להחליף את הסיסמה ליישומי הלמידה מרחוק אחת למספר חודשים. לשם הנוחות ניתן להשתמש בעניין זה במנגנון של מנהל סיסמאות.
- ודאו כי המחשב הביתי (הנייח או הנייד) בו אתם משתמשים בעת תהליך הלמידה מרחוק כולל מערכת הפעלה מעודכנת ותוכנת Anti-Virus פעילה. ודאו גם כי הרשת הביתית בה נעשה שימוש מאובטחת על ידי תוכנת חומת אש (Firewall) מעודכנת, וכי הרשת האלחוטית (Wi-Fi) בביתכם מוצפנת תחת סיסמה. במידה ואתם משתמשים בטלפון החכם ללמידה מרחוק – וודאו כי הטלפון שלכם מוגן בסיסמה או באמצעי זיהוי אחרים.
- בעת שימוש ביישומים דיגיטליים ללמידה מרחוק שאינם דורשים קיומו של שיח ויזואלי, הקפידו לכסות את המצלמה (בין אם מדובר במצלמת רשת או מצלמת המחשב או הטלפון הנייד) בכיסוי/מדבקה שתמנע את צילומכם על-ידי גורמים עבריינים העשויים להשתלט על המצלמה. ככלל, כדאי שמצלמות כאלה תהיינה מכוסות באופן קבוע, למעט כאשר אתם נדרשים להשתמש בהן.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

- ככלל, יישומים ללמידה מרחוק, ובמיוחד יישומים ציבוריים שאינם ייעודיים לשימוש תלמידים ושהשימוש בהם נעשה ללא רישיון הניתן בתשלום (שימוש "חינמי" לכאורה), עשויים לאסוף מידע רב על אודותיכם, לרבות כזה הנחשף על-ידכם במסגרת תהליך הלמידה. על כן הקפידו לא להעלות ולא לציין פרטים אישיים הנוגעים אליכם במסגרת הרישום או השימוש ביישומי למידה מרחוק (כגון כתובת המגורים או מספר הטלפון שלכם), אלא רק את הפרטים המינימאליים הנדרשים במסגרת הליך הלמידה עצמו.
- בחלק מהיישומים הטכנולוגיים ללמידה מרחוק עומדים למשתמשים כלים לשליטה, ולו חלקית, על אופן השימוש במידע שלהם. הקדישו זמן מה לשם למידת הכלים השונים והשתמשו בהם להגנה על פרטיותכם.

כך לדוגמה, לפי תנאי השימוש של Zoom, המערכת עושה שימוש במידע על משתמשים לשם שיפור פרסום מוצריה, ולשם כך מעבירה את המידע האישי של משתמשים לצדדים שלישיים, וזאת כברירת מחדל. משתמשים המבקשים למנוע את העברת המידע רשאים לבטל אפשרות זו ולשנות את ברירת המחדל באמצעות ביטול הסימון "sale" בהגדרת פרופיל המשתמש. כמו כן, רישום למערכת Zoom באמצעות חשבון הפייסבוק מאפשר למערכת גישה לנתוני פרופיל המשתמש בפייסבוק. רישום לשירותים מסוג זה באמצעות כתובת דואר אלקטרוני עשוי למנוע מצב זה.

- קחו בחשבון שכל מידע שתחשפו בעת שימושכם ביישומים ללמידה מרחוק הכוללים קיום שיח ויזואלי (כגון מערכות Zoom או Skype) עשוי להיות נגיש, מתועד ומצולם על-ידי גורמים אחרים המשתמשים ביישום. על כן, במסגרת השימוש ביישום הקפידו לא לחשוף את עצמכם ואת בני המשפחה שלכם, או פרטים העשויים לפגוע בפרטיותכם ובפרטיותם. מומלץ כי בכל שימוש מחדש ביישום של למידה מרחוק הכולל שיח ויזואלי תבחנו את סביבת האזור החשוף למצלמה ותוודאו כי אתם, ואחרים בביתכם, מרגישים בנוח עם פרטי המידע שייחשפו במסגרת הצילום. חשבו תמיד כיצד הדברים עשויים להיראות על-ידי משתמשים אחרים ביישום וודאו, לפי כל שימוש, כי אין באזור החשוף למצלמה משהו שאותו אתם, או בני ביתכם, לא תרצו שייחשף. תלמידים המבקשים לצמצם את חשיפת המרחב הפרטי שלהם במסגרת שיעורי למידה מרחוק הכוללים שיח ויזואלי יכולים לבחור באפשרות של שימוש ברקע וירטואלי, ככל שאפשרות זו קיימת מבחינה טכנולוגית ביישום.

מצד שני, כאשר אתם פועלים במסגרת יישומים ללמידה מרחוק הכוללים קיום שיח ויזואלי עם תלמידים אחרים, הקפידו לכבד את הפרטיות של שאר המשתמשים ביישום במקביל אליכם. במובן זה, אם במסגרת השימוש ביישום אתם נחשפים למידע אישי ופרטי של תלמיד אחר, הימנעו משמירת המידע וצילום המסך והקפידו שלא להעביר את התמונה או מידע הלאה. במקרים מתאימים רצוי לערב בעניין זה הורים ו/או גורמים רשמיים מטעם הגורם במסגרתו נערך תהליך הלמידה. בעניין זה יובהר כי פרסום או העברת צילום/סרטון אינטימי של אדם ללא הסכמתו ברשתות חברתיות (כגון WhatsApp),

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

מהווים עבירה פלילית. לעניין זה ראו סעיף 3(א)(5א) לחוק למניעת הטרדה מינית, התשנ"ח-1998.

- הקפידו לא לענות ולהגיב לגורמים שאינם חלק מתהליך הלמידה (כגון תלמידים אחרים) הפונים אליכם באופן אישי במסגרת השימוש ביישומי הלמידה מרחוק. במקרים הנחזים בעייתיים רצוי לערב הורים ו/או גורמים רשמיים מטעם הגורם במסגרתו נערך תהליך הלמידה.
- הקפידו לא להיכנס לקישורים שעשויים להישלח אליכם במסגרת השימוש ביישומי הלמידה מרחוק ולא להוריד קבצים הנשלחים אליכם במסגרת זו, אלא לאחר בדיקה כי קישורים אלו נשלחו אליכם מטעם גורמים מוסמכים וכחלק מתהליך הלמידה.
- מומלץ להורים לילדים בגילאים צעירים לתווך לילדיהם את הכללים השונים הנוגעים להגנה על פרטיותם, באופן כללי ותוך התייחסות לשימוש ביישומים ללמידה מרחוק, בפרט.

<u>דגשים והמלצות להתנהלות נכונה למוסדות חינוך, רשויות מקומיות, וגורמים נוספים שבמסגרתם מתקיימים תהליכי למידה מרחוק באמצעות יישומים טכנולוגיים</u>

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

- בעת הליך בחינת ובחירת זהות היישום הדיגיטלי 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.

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.

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

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

- ברמה העקרונית מומלץ לעשות שימוש ביישומים טכנולוגיים ייעודיים ללמידה מרחוק מאשר שימוש ביישומים ציבוריים-כללים שלא נועדו באופן ספציפי לשם כך.
- מומלץ כי השימוש ביישומים של למידה מרחוק 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, 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. בדומה, על מנת לשמור על פרטיות המשתתפים בפגישה יש לוודא שהאפשרות Attention Tracking כבויה, 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).
- 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). בכל מקרה רצוי שלא לשמור את החומרים בחשבונות המנוהלים ב"עננים" ציבוריים, כגון Dropbox.
- מומלץ כי עם המעבר למסגרת של למידה מרחוק יובהרו ויחודדו למשתמשים ביישומים, לרבות תלמידים ועובדי ההוראה, הכללים השונים הנוגעים להתנהלות במסגרת יישומים

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

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.

- בכל הנוגע לאפשרות לצלם שיעור המתקיים בכיתה עם תלמידים, לצורך השתתפות של חלק מהתלמידים בלמידה מרחוק, נציין כי חוזר מנכ"ל משרד החינוך אוסר על הצבת מצלמות בכיתות הלימוד.[5]

- 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 לבצע על מנת להקטין סיכון להתקיימות אירועי אבטחת מידע ופגיעה בפרטיות. להרחבה בנוגע להיבטים של הגנה על פרטיות בהפעלת מדיניות של עבודה מרחוק, ראו מסמך של הרשות להגנת הפרטיות בקישור הבא:

https://www.gov.il/BlobFolder/reports/corona_work/he/WORK%D6%B9PRIVACY%D6%B9CORONA.pdf

- מומלץ שמוסדות חינוך יפעלו להנגשת ולהטמעת ההמלצות להגנה על פרטיות ולהתנהלות מיטבית ובטוחה ביישומים השונים ללמידה מרחוק, אשר פורטו קודם לכן, בקרב תלמידים והורים. מודעות לסוגית הפרטיות היא קריטית לשם ההגנה עליה.

---

[5] סעיף 2.24 לחוזר מנכ"ל משרד החינוך מס' 119 "מצלמות במוסדות חינוך – הסדרת הכנסתן ואופן התקנתן" (3.5.2015), https://apps.education.gov.il/mankal/horaa.aspx?siduri=134.

- מומלץ לעשות שימוש בכלים הנלווים המסופקים עם יישומי הלימוד מרחוק 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 מרחוק מומלץ להגביר את הניטור והפיקוח על פעילות היישומים הטכנולוגיים והחברות במסגרתם הם פועלים, וזאת בין היתר בכל הנוגע לעמידה בכללי אבטחת מידע. על סוגיה זו יורחב בחלק הבא.

<u>כללי אבטחת מידע למוסדות חינוך, רשויות מקומיות, ולגורמים נוספים שבמסגרתם מתקיימים תהליכי למידה מרחוק באמצעות יישומים טכנולוגיים</u>

כל גורם, ציבורי או פרטי, שבבעלותו מאגר מידע כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981, מחויב על פי דין בעמידה בכללים שונים הנוגעים לאבטחת המידע שבמאגר. כללים אלו מפורטים בחוק הגנת הפרטיות ובתקנות שהותקנו מכוחו, לרבות תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "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. 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.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

הרשות להגנת הפרטיות פרסמה מספר המלצות לנושאים אותם ראוי לעגן 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

סיכום

שנת הלימודים הנפתחת בקרוב צפויה להיות מורכבת וזאת, בין היתר, בשל הצורך של מוסדות חינוך לשלב בין מודל של למידה "מסורתית" בכיתות הלימוד למודל של למידה מרחוק, בהתאם להנחיות משרד החינוך בנושא. במציאות המורכבת בה אנו נמצאים, ההחלטה על מעבר תלמידים בשלבי חינוך שונים ללמידה במודל של למידה מרחוק היא מתבקשת. עם זאת יש להכיר בכך שלהחלטה זו עשויה להיות השלכה על פרטיותם של תלמידים רבים, לרבות מבחינת ההגנה על מידע הנוגע אליהם. לפיכך, על כל הגורמים הרלוונטיים לפעול בעניין באחריות ותוך הקפדה על עקרונות הגנת הפרטיות וההגנה על המידע.

במסמך זה התייחסנו להיבטים של פרטיות בלמידה מרחוק. להתייחסות נרחבת יותר מטעם הרשות להגנת הפרטיות בנושאי הגנת פרטיות במצב הנוכחי, הכולל פירוט של שאלות ותשובות, ראו:

https://www.gov.il/he/departments/faq/coronavirus_qa

הרשות להגנת הפרטיות הקימה "קו חם" לסיוע במתן פתרונות מעשיים, ישימים ומהירים בתחומי פרטיות, וצוות הרשות זמין בכל עת למתן פתרונות בנושאי פרטיות ועיצוב פתרונות תומכי פרטיות בכל נושא הרלוונטי לפעילות החירום בעת הזו. יודגש כי פתרונות ישימים אלה יינתנו על ידי הרשות בלוחות זמנים קצרים ביותר כמתבקש בנסיבות.

ניתן לעמוד עמנו בקשר דרך עמוד הפייסבוק של הרשות ("הרשות להגנת הפרטיות") או במייל: ppa@justice.gov.il

נשמח לעמוד לרשותכם בכל נושא ועניין ולספק מענה לשאלותיכם. לשאלות והרחבות בעניינים אלו ואחרים בקרו באתר האינטרנט של הרשות להגנת הפרטיות:

https://www.gov.il/he/departments/the_privacy_protection_authority