12 אוקטובר 2023
כז' בתשרי התשפ"ד

הגנת פרטיות תלמידים בלמידה מקוונת מרחוק

נוסח מעודכן בעקבות תיקון 13

רקע

במציאות הישראלית מתעוררים לעיתים מצבים בהם תלמידים (מכלל הגילאים ושלבי החינוך) נדרשים להעביר חלק מזירת הפעילות הלימודית שלהם מספסלי הלימודים לביתם הפרטי.

'**למידה מקוונת מרחוק**' היא מסגרת של למידה הנערכת באופן מקוון בעבור תלמידים הנמצאים מחוץ לכותלי המוסד החינוכי. 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.

למעבר למודל של למידה מקוונת מרחוק עשוי להיות השלכה דרמטית על פרטיות תלמידים, לרבות מבחינת ההגנה על מידע אישי הנוגע אליהם. יישומים דיגיטליים ללמידה מקוונת 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 מקוונת 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 שיעשו בו שימוש לרעה. חשיפה שכזו עשויה להיגרם גם כתוצאה מפעילות גורמים אחרים המקיימים אינטראקציות עם תלמידים על גבי היישומים האמורים, כגון מורים ותלמידים אחרים.

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 השיעורים שנערכו מרחוק בתקופת ההתמודדות עם נגיף הקורונה, עלו טענות מצדם של תלמידים כי חיוב זה פוגע בפרטיותם.

מטרת המסמך היא להציג מספר דגשים והמלצות להתנהלות נכונה ולהגנה על פרטיות ומידע אישי במסגרת שימוש תלמידים ביישומי למידה מקוונת מרחוק.[1] המסמך כולל דגשים והמלצות להורים ולתלמידים, דגשים והמלצות לגורמים המקיימים תהליכי למידה מקוונת מרחוק (כגון מוסדות חינוך, רשתות חינוך ורשויות מקומיות), דגשים והמלצות בלמידה משולבת (היברידית), ותמצות של כללי אבטחת מידע מרכזיים בנושא.

<u>למידה מקוונת מרחוק - דגשים והמלצות להתנהלות נכונה להורים ותלמידים</u>

למשתמשים ביישומים הדיגיטליים ללמידה מקוונת 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:

- השתמשו בסיסמאות חזקות למחשב וליישומי הלמידה המקוונת 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 המקוונת מרחוק אחת למספר חודשים. לשם הנוחות ניתן להשתמש בעניין זה במנגנון של מנהל סיסמאות.
- ודאו כי המחשב הביתי (הנייח או הנייד) בו אתם משתמשים 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 מקוונת 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.

[1] להרחבה בנושא פרטיות בלמידה מרחוק ובנושא פרטיות תלמידים בכלל ראו מדריך הרשות להגנת הפרטיות "פרטיות תלמידים במוסדות חינוך בעידן הדיגיטלי" (נובמבר 2021), (להלן: 'מדריך פרטיות תלמידים'): https://www.gov.il/he/pages/students_privacy_guide.

- ככלל, יישומים ללמידה מקוונת 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 הלמידה מרחוק (כגון כתובת המגורים או מספר הטלפון שלכם), אלא רק את הפרטים המינימאליים הנדרשים במסגרת הליך הלמידה עצמו.

- בחלק מהיישומים ללמידה מקוונת מרחוק עומדים למשתמשים כלים לשליטה, ולו חלקית, על אופן השימוש במידע שלהם. הקדישו זמן מה לשם למידת הכלים השונים והשתמשו בהם להגנה על פרטיותכם.

- קחו בחשבון שכל מידע שתחשפו בעת שימושכם ביישומים ללמידה מקוונת מרחוק הכוללים קיום שיח ויזואלי 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.

- הקפידו לכבד את הפרטיות של שאר המשתמשים ביישום במקביל אליכם. 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), מהווים עבירה פלילית. לעניין זה ראו סעיף 3(א)(5א) לחוק למניעת הטרדה מינית, התשנ"ח-1998.

- 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 צעירים לתווך לילדיהם את הכללים השונים הנוגעים להגנה על פרטיותם, באופן כללי ותוך התייחסות לשימוש ביישומים ללמידה מרחוק, בפרט.

<u>למידה מקוונת מרחוק - דגשים והמלצות למוסדות חינוך, רשתות חינוך ורשויות מקומיות</u>[2]

להלן פירוט דגשים לגורמים המבקשים להפעיל תוכניות ללמידה מקוונת 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 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 מקוונת 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 מוסדות חינוך, רשתות חינוך ורשויות מקומיות המבקשים להשתמש ביישומים טכנולוגיים ללמידה מקוונת מרחוק יפעלו מול הגורמים הרלוונטיים במשרד החינוך על מנת לוודא כי היישום בו הם מבקשים לעשות שימוש מאושר על-ידי המשרד, וכי הוא עומד בהקשר זה בכל כללי אבטחת המידע הנדרשים ע"פ הוראות הדין.

- מומלץ כי השימוש ביישומים ללמידה מקוונת מרחוק יעשה במסגרת של רכישת רישיון לשימוש ביישומים אלו. 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.

- 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

[2] ההמלצות המפורטות בחלק זה רלוונטיות גם לגורמים נוספים המקיימים תהליכי למידה מקוונת מרחוק כגון תנועות נוער וכדומה.

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 ב"עננים" ציבוריים, כגון Dropbox.
- מומלץ כי עם המעבר למסגרת של למידה מקוונת מרחוק יובהרו ויחודדו למשתמשים ביישומים, לרבות תלמידים ועובדי ההוראה, הכללים השונים הנוגעים להתנהלות במסגרת יישומים אלו, לרבות בנוגע להגנה על הפרטיות המשתתפים בשיעור.
- 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,[3] וכי נכון למועד כתיבת מסמך זה לא ניתנה הנחיה מטעם משרד החינוך לחיוב תלמידים בפתיחת מצלמות.

[3] סוגיית חיוב תלמידים בפתיחת מצלמות במהלך שיעורים נמצאת כיום בהליכי הסדרה במסגרת הנחיות משרד החינוך. ככלל, ככל הידוע לרשות, משרד החינוך רואה חשיבות רבה בשימוש בווידאו ובשמע על ידי התלמידים במסגרת הלמידה

- 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.[4]
- מומלץ שמוסדות חינוך יפעלו להנגשת ולהטמעת ההמלצות להגנה על פרטיות ולהתנהלות מיטבית ובטוחה ביישומים השונים ללמידה מקוונת מרחוק בקרב תלמידים והורים.[5] 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.

<u>למידה משולבת (היברידית) -דגשים והמלצות למוסדות חינוך, רשתות חינוך ורשויות מקומיות</u>[6]

למידה מקוונת 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:[7]

המקוונת מרחוק. 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.

[4] להרחבה בנוגע להיבטים של הגנה על פרטיות בהפעלת מדיניות של עבודה מרחוק ראו https://www.gov.il/he/pages/corona_work.

[5] למיטב ידיעת הרשות, משרד החינוך מפעיל תכנית מערכתית להתנהלות מיטבית ברשת, הכוללת גם התייחסות להיבטים של שמירת הפרטיות. ראו: https://meyda.education.gov.il/files/shefi/glishabetuha/Tochnit_Maarachtit_Mekuzar.pdf.

[6] 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. למיטב ידיעת הרשות, בימים אלה נבחנת במשרד החינוך מדיניות המאפשרת למידה משולבת גם בגני ילדים.

[7] חלק זה מבוסס על הנחיות משרד החינוך להעברת שיעור בלמידה משולבת https://meyda.education.gov.il/files/edu/photo-in-class.pdf. להרחבה בנושא זה ראו גם מדריך פרטיות תלמידים, לעיל ה"ש 1, עמ' 57-58.

- 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.
- צילום שיעור מרחוק בזמן אמת יעשה על-ידי המורה באמצעות המצלמה המובנית שבמחשב בו עושה המורה שימוש; המצלמה המחוברת למחשב שברשות המורה; או המצלמה שבמכשיר הטלפון של המורה.
- 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, שהמצלמה 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 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. האיסור חל גם על העברת הקישור לשיעור או הסיסמה לכניסה אליו.
- ככלל, אין לשמור צילום או הקלטה של שיעור. במקרים חריגים בהם קיים צורך לשמור צילום/הקלטת שמע לשם העברת השיעור לתלמידים שלא יכלו לצפות בשיעור בזמן אמת, מורה רשאי לשמור את הקלטת השיעור לשם העברתה לתלמידים האמורים. על המורה להקפיד על כללים שונים הנוגעים לאבטחת המידע. לדוגמה, על המורה לוודא שהקישור 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 שאושרו על-ידי משרד החינוך. בעניין זה יובהר כי אין

לשמור את החומרים המצולמים בחשבונות פרטיים, ואין לפרסם את השיעורים בפלטפורמות ציבוריות כגון YouTube.

- המורה ימחק את ההקלטה עד שבוע ימים מיום העברת ההקלטה, לכל המאוחר.

סיכום

במצבים מסוימים, ההחלטה על מעבר תלמידים בשלבי חינוך שונים ללמידה במודל של למידה מקוונת מרחוק עשויה להיות 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 ואבטחת מידע על אודות תלמידים.[8]

[8] להרחבה בנושא כללי אבטחת מידע ראו תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, וכן עמודים 25-31 למדריך פרטיות תלמידים, לעיל ה"ש 1.