**מדינת ישראל**
**משרד החינוך**
**מינהל תקשוב טכנולוגיה ומערכות מידע**

# מדיניות שמירה וטיפול במידע מוגן במוסדות חינוך

**1. מבוא:**

במהלך העבודה בבית הספר נעשה שימוש במידע אודות עובדי הוראה, תלמידים ומשפחותיהם אשר חשיפתו לגורמים לא מורשים עלול לגרום נזק ועבירה על חוק הגנת הפרטיות. מסמך זה מפרט כיצד יש לטפל במידע מסוג זה.

2. **הגדרות:**

מידע מוגן – נתונים על אישיותו של אדם, צנעת אישיותו, מצב בריאותו, מצבו הכלכלי, הכשרתו המקצועית, דעותיו ואמונתו. למען הסר ספק מובהר, כי גם נתונים כאמור על קטין, כמו נתונים על מבוגר, ייחשבו כ"מידע", וכך גם נתונים אשר לכשעצמם אינם "מידע" אולם הם מוחזקים תחת כותרת שאפשר ללמוד ממנה על מידע כאמור (למשל, רשימת שמות של הורי תלמידים המוחזקת תחת הכותרת "הורים המצויים במצב כלכלי קשה" וכדומה).

**3. הנחיות:**

**א. כללים לשמירת מידע מוגן**

**מידע מוגן ניתן לשמור במקומות הבאים:**

- מערכות משרד החינוך
- מוצרים חינוכיים טכנולוגיים מאושרים על ידי משרד החינוך עמם יש למוסד החינוכי התקשרות. להלן קישור לרשימת הספקים המורשים ב"קטלוג החינוכי".
- בספריות רשת ייעודיות בשרת בית הספר.
- סביבות ענן בית ספריות מסוג Microsoft Office 365 for Education.

**אין לשמור מידע מוגן ב:**

- מחשבים פרטיים (כגון מחשבים ביתיים עליהם מתבצעת עבודה).
- התקנים ניידים (כגון Disk on key).
- מחשבי בית ספר ברשת הפדגוגית.
- מחשבי בית ספר ציבוריים בהם עושים שימוש משתמשים שונים.
- חשבונות ענן פרטיים.

**ב. הפרדה וניהול הרשאות גישה**

יש להקפיד כי במקומות בהם נעשה שימוש לשמירת מידע מוגן תבוצע באמצעות הרשאות גישה שונות לאנשי הצוות. לדוגמא בשרת הבית ספרי תוקצה ספריה ייעודית לכל בעל תפקיד. הרשאות הגישה לספריות אלו ינוהלו כך שרק לבעלי התפקידים הרלבנטיים תהיה גישה למידע באזור זה. כך למשל יש להקצות ליועצת בית הספר ספריית רשת נפרדת אשר רק לה תהיה גישה לתכניה.

**חשוב: אין לאפשר עבודת תלמידים על מחשבים ברשת המנהלתית ואין לאפשר גישת תלמידים למקומות בהם נשמר מידע מוגן**

**ג. טיפול במידע מוגן**

יש להקפיד על הכללים הבאים בעת שימוש/טיפול במידע מוגן:

- אין להציג מידע מוגן בסביבה פומבית בה נוכחים גורמים בלתי מורשים
- אין להשאיר מידע מוגן או סיסמאות גישה למידע מוגן באזורים להם יש גישה לגורמים בלתי מורשים

- מידע מודפס: יש להקפיד על כך שמסמכים מודפסים המכילים מידע מוגן לא יישארו חשופים באזורים פומביים (למשל על מגש המדפסת) לאורך זמן. יש לתייק את המסמכים בארונות או חדרים אותם ניתן לנעול ולגרוס את המסמכים עם סיום השימוש.
- העברת מידע: אין לעשות שימוש בחשבונות פרטיים כגון דוא"ל פרטי, תוכנות מסרים מיידים וכד' לצורך העברת מידע מוגן. יש לעשות זאת באמצעות האמצעים אותם מעמיד בית הספר לשימוש כגון דוא"ל בית ספרי ושירותי ענן בית ספריים.

**<u>חשוב</u>**: על מנת למנוע טעויות – יש לוודא לפני ביצוע השליחה כי הכתובת אליה נשלח המידע מדויקת וכי הגורם המקבל מורשה לטפל במידע זה.

**ד. טיפול באירוע זליגת מידע מוגן**

במידה והתגלה כי גורם לא מורשה נחשף למידע מוגן יש לבצע את הפעולות הבאות:

- לבטל את הפעולה אם ניתן – למשל משיכת דוא"ל שנשלח, ביטול הרשאה לספריה בענן וכדומה.
- ליידע את מנהל/ת בית הספר בהקדם האפשרי.
- ליידע את משרד החינוך בכתובת הדוא"ל:

school_security@education.gov.il