

Indicazioni e accorgimenti privacy in ambito di lavoro smart e didattica e-learning

Il presente documento si intende quale supporto operativo all'attività degli Istituti scolastici, relativamente al corretto trattamento dei dati personali nelle modalità e-learning per la didattica, che dovranno avvenire secondo le linee guida e le istruzioni fornite dal Ministero dell'Istruzione, dall'Intendenza scolastica di riferimento nonché dalla Dirigenza.

La modalità di didattica a distanza rappresenta ormai una realtà operativa necessaria per gli istituti scolastici, al fine di garantire agli alunni e agli studenti la continuazione degli studi e dell'apprendimento. Per trarre il massimo vantaggio da questa opportunità, generata da eventi del tutto straordinari, occorre però dare la giusta attenzione ad aspetti non certo secondari, quali la sicurezza dei dati personali e delle informazioni.

Lo scopo del presente documento è fornire indicazioni accorgimenti in relazione allo svolgimento dell'attività lavorativa nonché dell'attività didattica in remoto: tale modalità di lavoro si era presentata in passato solamente in casi sporadici, dunque la finalità delle presenti indicazioni è quella di porre la necessaria attenzione ai risvolti di sicurezza e all'uso di strumenti idonei, per non mettere a rischio né i dati degli studenti né degli stessi docenti.

Sicurezza dell'informazione: attenzione al data breach!

Chiaramente, l'attività lavorativa e didattica svolta in un luogo che normalmente non è adibito a tale funzionalità (come il domicilio) comporta di per sé un aumento importante delle minacce a cui i dati personali e le informazioni in generale sono sottoposti. Ricordiamo che qualsiasi *"violazione di sicurezza che comporti accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"* si configura come una violazione di dati personali. Tale violazione può accadere sia accidentalmente che di proposito: i dati personali subiscono un trattamento non voluto e non preventivato dal Titolare del trattamento (Istituto Scolastico) e che le misure di sicurezza adottate non hanno potuto evitare. Questo può avvenire sia a causa di comportamenti dolosi di terzi che a seguito di un semplice errore da parte di una persona autorizzata al trattamento degli stessi.

Esempi di data breach: perdita, distruzione o furto di documenti cartacei e/o digitali, casi di pirateria informatica, divulgazione di dati confidenziali a persone non autorizzate,

Sicurezza dei dati e delle informazioni su supporto informatico

Il tema è molto complesso, ma possiamo affermare, sulla base della nostra esperienza, che la maggiore criticità sia data dall'utilizzo dei dispositivi personali per accedere al sistema informatico della scuola, ivi incluse le connessioni di rete (ADSL, WiFi, ecc.) dove magari non si sono modificati i parametri standard (come ad esempio le password).

Molto spesso a casa siamo portati a trascurare le misure di sicurezza più basilari come antivirus/antimalware e si sottovalutano i piccoli rischi connessi ad una navigazione ingenua. La possibilità che i computer abbiano malware già attivi è uno scenario seriamente pericoloso e con una probabilità molto alta.

Ecco alcuni suggerimenti pratici:

- Installare un buon sistema di antivirus
- Scaricare un sistema di gestione remota del PC (come ad esempio piattaforme Kaseya, Solarwind, ManageEngine o Teamviewer), per facilitare l'assistenza da parte del personale preposto;
- Mantenere riservate le credenziali di autenticazione a sistemi e software (nome utente e password), che sono da considerarsi assolutamente riservate e personali.

Attenzione alla diffusione di malware inerenti al Covid 19!

Vi sono purtroppo nuove minacce informatiche, che sfruttano la tematica del coronavirus e l'attenzione che la tematica risveglia in tutti noi. In particolare, la polizia postale segnala due malware diffusi via e-mail attraverso comunicazioni spa, che potrebbero interessare anche le caselle di posta istituzionale, inducendo in errore gli operatori. Si tratta di allegati in apparenza .pdf e allegati .doc recanti titoli simili a "CoronavirusSafetyMeasures", allegati ad e-mail spam: tali file avviano

il download di contenuti spazzatura. Si suggerisce dunque di porre estrema cautela anche nella gestione ordinaria della propria posta elettronica istituzionale, evitando di aprire tali allegati qualora l'e-mail risulti sospetta (ad esempio, il sospetto può derivare da un mittente non riconosciuto; dall'inclusione in una lista di destinatari con numerosissimi indirizzi e-mail non riconosciuti; o per la modalità di scrittura che presenta numerosi errori grammaticali nonché l'utilizzo di caratteri non comuni all'alfabeto italiano; ecc.).

Riguardo al supporto informatico di riferimento e alle piattaforme e-learning

Relativamente alle piattaforme da utilizzare per la didattica e-learning, il suggerimento è fare riferimento alle piattaforme indicate dal Ministero dell'Istruzione sul sito Internet istituzionale, da cui riportiamo a titolo esemplificativo "Teams" di Microsoft, che consente la partecipazione alla videoconferenza di molte persone, strumento adatto quindi anche alle classi numerose, oltre a consentire la registrazione della lezione.

Nel momento della videoconferenza, può essere opportuno da parte del docente ricorrere a soluzioni di "appello digitale", al fine di verificare l'effettiva presenza dei soli alunni partecipanti, facendo inoltre attenzione all'utilizzo da parte dell'alunno di indirizzi non propri (di genitori o altri familiari).

Anche per lo stesso docente, qualora effettui un invio di documentazione ai propri studenti mediante comunicazione e-mail (se tale modalità è permessa dal Dirigente), la conformità al corretto trattamento dei dati suggerisce l'utilizzo esclusivo della propria e-mail lavorativa; si consiglia inoltre di prediligere l'invio della documentazione in copia conoscenza nascosta ai destinatari determinati.

Per le comunicazioni ufficiali da parte della scuola, lo strumento da prediligere è il registro elettronico.

Sicurezza dei dati e delle informazioni su supporto cartaceo

Qualora si sia valutato come necessario avere a disposizione documentazione cartacea al di fuori dei locali scolastici, si deve tener conto, come avviene nel caso del supporto informatico, la c.d. terna RID:

- Riservatezza
- Integrità
- Disponibilità

Qualora venisse a mancare una di queste caratteristiche della sicurezza delle informazioni siamo in presenza di una violazione di tali informazioni. Si raccomanda quindi di conservare i documenti cartacei con la massima cura, riponendoli in raccoglitori dedicati, teche, cassette (ove possibile) avendo cura che i documenti e le informazioni ivi contenute non siano accessibili a soggetti terzi non autorizzati (es. familiari, conviventi etc.). In caso di necessità di distruzione di documenti, si suggerisce di avvalersi di un distruggi documenti. Ove non disponibili, si suggerisce di raccogliere e archiviare la documentazione in modo ordinato, così da poterla distruggere una volta rientrati in azienda, ove saranno disponibili i distruggi documenti necessari alla corretta distruzione degli stessi.

Qualora nonostante l'adozione degli opportuni accorgimenti e di costante attenzione al trattamento di dati personali dovesse avvenire un "data breach", vi è la necessità di contattare senza ingiustificato ritardo il proprio Dirigente, il quale si metterà in contatto con il DPO, per la valutazione circa gli adempimenti normativamente previsti; tali adempimenti consistono in:

- Comunicazione al Garante Privacy mediante l'apposita procedura online (entro 72 dalla presa coscienza dell'evento! È necessaria una pronta reazione)
- Comunicazione agli interessati, secondo la modalità valutata più idonea nel caso concreto

In conclusione

Quello che ci viene dunque richiesto in questo momento particolare, è un'attenta analisi dei rischi riguardante la sicurezza delle informazioni trattate e applicazione delle best practises nel mondo scolastico, già applicate alla realtà operativa della didattica in presenza, adattate al mondo digitale, facendo attenzione alle indicazioni e agli accorgimenti sopra indicati.

Il team DPO resta a disposizione per ogni necessità o ulteriore approfondimento.

#andràtuttobene