Linee guida di utilizzo della piattaforma G-Suite for Education

Morolabs Srl
[NOME DELLA SOCIETÀ]

Sommario

Premessa

Le piattaforme per la Didattica Digitale Integrata (d'ora in poi anche "DDI") offrono molte funzionalità, dalla videoconferenza all'archiviazione, dalla posta elettronica alla gestione dei moduli on-line.

Considerando gli utilizzi ordinari delle piattaforme DDI in ambito scolastico, a meno di specifiche limitazioni sul numero di utenze contemporanee, le versioni gratuite o a pagamento tendono a risultare praticamente identiche, cosicché la maggioranza degli istituti predilige le prime, tenendo conto delle esigue risorse economiche solitamente a disposizione degli stessi.

La scelta delle versioni gratuite potrebbe però nascondere numerose insidie dal punto di vista della protezione dei dati personali, talvolta anche particolari, degli allievi o comunque influenzarli fin dai primi passi digitali nella preferenza dell'uno o dell'altro fornitore di servizi IT, in funzione, magari, delle scelte effettuate dall'Istituto scolastico frequentato.

Nell'attuale scenario di piena emergenza pandemica, viste le indifferibili esigenze di didattica digitale, appaiono del tutto secondari i problemi legati ai meccanismi di fidelizzazione da parte dei fornitori del prodotto/servizio nei confronti dell'utenza; risulta tuttavia doveroso, però, tentare di ridurre i rischi legati al trattamento dei dati personali, potenzialmente anche di tipo particolare, secondo quanto disposto dalla normativa vigente (Regolamento (UE) 2016/679 o GDPR), basandosi sui principi e applicando tecniche come la minimizzazione, la pseudonimizzazione o operando in maniera preventiva secondo la *privacy by design*.

Le indicazioni pratiche che seguono sono volte a ridurre la superficie di esposizione rispetto al trattamento dei dati personali dei ragazzi e del personale docente, in modo che nessuno possa, anche in futuro, sfruttare le informazioni acquisite per altre finalità.

Principi cardine sulla protezione dei dati personali

L'Articolo 5 del GDPR delinea i seguenti principi base della protezione dei dati personali:

1. Liceità, correttezza e trasparenza
2. Limitazione della finalità
3. Minimizzazione dei dati
4. Esattezza
5. Limitazione della conservazione
6. Integrità e riservatezza

Il legislatore europeo, in modo più esplicito rispetto alla precedente direttiva 95/46, ha proclamato, con il GDPR, la tutela del diritto alla protezione dei dati personali inteso come diritto fondamentale delle persone fisiche nella società dell'informazione; la declinazione dei principi e delle sottese tecniche di protezione, permette ad ogni cittadino europeo di trattare dati personali in piena conformità normativa.

La liceità del trattamento dei dati personali svolto dall'Istituto ed effettuato tramite piattaforme di DDI è garantita in quanto connessa *"all'esecuzione di un compito di interesse pubblico di cui è investita la scuola attraverso una modalità operativa prevista dalla normativa, con particolare riguardo anche alla gestione attuale della fase di emergenza epidemiologica*" [Didattica Digitale Integrata e tutela della privacy: indicazioni generali – Gruppo di lavoro congiunto Ministero dell'istruzione-Ufficio del Garante per la protezione dei dati personali].

Così come previsto nel Provvedimento del 26 marzo 2020, n. 64 (doc web n. 9300784 "Didattica a distanza: prime indicazioni") non è quindi necessario richiedere uno specifico consenso *privacy* ai genitori per l'utilizzo delle piattaforme nella didattica degli allievi.

Nelle varie informative relative alla piattaforma G Suite, Google ha sempre definito come buona prassi la richiesta ai genitori o tutori dell'*autorizzazione all'uso dei Servizi principali attivati dalla scuola* che può essere acquisita attraverso un semplice segno di spunta in un form all'interno del registro elettronico evitando dunque moduli cartacei, così come previsto anche dalle disposizioni nazionali sulla digitalizzazione.

Sempre relativamente al primo punto e in particolare ai temi di "correttezza e trasparenza" è necessario far riferimento all'informativa generale con particolare riguardo all'utilizzo delle piattaforme DDI dove sono indicate le finalità, le modalità di trattamento e soprattutto le cosiddette "regole del gioco".

La "Limitazione della finalità" è un punto centrale della normativa: non è possibile acquisire dati personali per una determinata finalità ed utilizzarli per procedere ad ulteriori trattamenti o in funzione di altri obiettivi inizialmente non previsti nelle informative.

Questo principio è valido anche nella catena di relazioni tra titolare, responsabili e sub-responsabili; nello specifico, il fornitore di un servizio o di una piattaforma, che effettua trattamenti nel ruolo di responsabile del trattamento, non può utilizzare i dati acquisiti per svolgere altre attività o perseguire ulteriori obiettivi rispetto a quanto autorizzato dal titolare.

Esiste però un problema di controllo dei contenuti: un conto è l'utilizzo delle piattaforme con lo scopo di distribuzione dei materiali didattici e degli esercizi agli allievi; questione del tutto differente, invece, è ad esempio la condivisione tra colleghi di relazioni BES, diagnosi DSA o PDP. In quest'ultimo caso i rischi sono molteplici e non solo legati alla (remota?) possibilità per il motore di ricerca più potente al mondo di effettuare analisi o indicizzazioni sui contenuti ma rispetto a possibili accessi non autorizzati o, più semplicemente, ad una condivisione malriuscita ed erroneamente rivolta ad un pubblico più ampio del previsto.

A prima vista, considerata la facilità di utilizzo e la comodità degli strumenti disponibili nelle piattaforme, non sussistono particolari differenze tra il caricamento di una serie di esercizi, necessari per evidenti finalità didattiche, e la condivisione di informazioni relative ad un soggetto particolarmente fragile, utili, invece, per la personalizzazione da parte dei componenti del consiglio di classe del relativo piano individuale. L' all'esposizione ai rischi dei dati trattati nelle due situazioni è totalmente differente.

Fin troppo spesso si disseminano contenuti a partire dai nomi dei file o delle cartelle; è un modo facile per rendere più agevole l'accesso agli autorizzati ma, non avendo pieno controllo degli strumenti utilizzati, è preferibile procedere, anche in questi casi apparentemente banali, con la massima cautela.

La "Minimizzazione dei dati" è un principio oltre che una delle tecniche utilizzate per ridurre la superficie di esposizione e conseguentemente diminuire il livello di rischio incombente sui dati. Trattare soltanto un insieme minimo di informazioni effettivamente utili permette di evitare che, al contrario, un eventuale surplus esponga i soggetti, anche solo potenzialmente, a problematiche legate ai loro diritti, alla loro dignità, alla loro libertà. È fondamentale iniziare a pensare in termini di necessità, ovvero al trattamento dei soli dati essenziali per il perseguimento delle finalità con la conseguente riduzione dei rischi legati alle attività svolte.

La facilità di utilizzo di certi strumenti del web mal si coniuga con i controlli effettuati dagli applicativi software sull'immissione o modifica dei dati. Mentre in alcuni applicativi è impossibile procedere con la cancellazione di una registrazione, lo stesso non si può affermare in relazione agli strumenti di produttività individuale, come ad esempio i fogli elettronici che permettono qualsiasi modifica, praticamente senza lasciare tracce.

Garantire quindi la dovuta esattezza delle informazioni non è soltanto un dovere morale ma un obbligo normativo oltreché un elemento in grado di infondere nei cittadini la necessaria fiducia nella società digitale (che verrà). Sbagliare una valutazione, un risultato o peggio un esito non è un problema di poco conto specie se per colpa di una riga cancellata in un foglio elettronico.

Il comportamento di molti utilizzatori non è sicuramente incentrato nella razionalizzazione degli spazi di memoria. Questo non è tendenzialmente un problema nei sistemi personali per la crescita esponenziale degli spazi ma lo può diventare per la protezione dei contenuti.

La riduzione dell'esposizione non è soltanto un problema che riguarda la superficie di esposizione (quantità di dati) ma deve essere intesa anche in termini temporali.

Limitare i tempi di conservazione dei dati personali, oltre che un principio, è una tecnica adottabile proprio al fine di evitare a monte eventuali problemi; alcuni utilizzatori diventano nel tempo degli accumulatori seriali di file di tutti i tipi, contenenti milioni di informazioni, contando su un improbabile utilizzo futuro.

Conservare indefinitamente delle informazioni una volta terminata la finalità aumenta soltanto il numero di persone potenzialmente danneggiate da un *data breach* e la mole di dati forniti al soggetto attaccante. Di contro, non sussistono, ovviamente, obblighi di protezione per chi non possiede informazioni.

Per queste motivazioni è necessario conservare soltanto quanto effettivamente necessario e per il solo tempo previsto dai massimari di conservazione; prima dell'avvento della digitalizzazione era previsto lo scarto di archivio per evidenti difficoltà legate ai limitati spazi destinata all'archiviazione. Oggi questo non succede poiché l'utilizzatore di questi strumenti non percepisce limitazioni negli spazi di memoria (seppur esistenti) e non provvede alla distruzione che rappresenta l'unico vero meccanismo di messa in sicurezza delle informazioni.

Una volta terminata l'attività, l'anno o il ciclo scolastico, dovrà essere cura di ogni singolo operatore procedere all'eliminazione dei file relativi al trattamento conclusosi per la specifica finalità.

La riservatezza è il diritto alla non intromissione nella sfera individuale della persona da parte di soggetti non autorizzati. È evidente come la garanzia di tale diritto sia fortemente legata all'applicazione di logiche di definizione di profili di autorizzazione agli accessi in funzione dei ruoli ricoperti e delle funzioni espletate.

Accessi indiscriminati non sono accettabili in nessun contesto; è quindi necessario definire all'interno della piattaforma almeno due tipologie di soggetti: amministratori della piattaforma e utilizzatori, volendo con ulteriori livelli di stratificazione. In aggiunta è necessario suddividere l'appartenenza a gruppi legati ad esempio ai consigli di classe o ai diversi progetti del PTOF per definire i profili di autorizzazione.

Riuscire a garantire la dovuta integrità delle informazioni può apparire un elemento esclusivamente legato alle tecnologie, in realtà è un problema relativo ai profili di autorizzazione nonché alla riduzione della possibilità per gli utilizzatori di combinare guai. La tutela dell'accuratezza, la completezza dei dati così come la protezione da alterazioni e danneggiamenti devono essere un obiettivo condiviso da tutti poiché legato alla continuità operativa dei servizi e all'autorevolezza delle informazioni sulla base delle quali sono prese le relative decisioni.

Applicazione pratica dei principi cardine

L'applicazione pratica dei suddetti principi cardine del Regolamento riguarda le dimensioni di seguito elencate e specificatamente descritte nei prossimi paragrafi:

1. Identità digitale e profili di autorizzazione
2. Credenziali di autenticazione
3. Registrazione delle attività (Accounting)
4. Tipologia di dati trattati rispetto alle finalità previste
5. Tecniche di protezione (modalità condivisione e invio)
6. Tempistiche di conservazione
7. Dispositivi utilizzati (BYOD), a scuola e a casa

Identità digitale e profili di autorizzazione

La piattaforma implementa la famiglia di protocolli detti AAA ovvero basati sulle funzioni di Autenticazione, Autorizzazione, Accounting.

L'accesso alla rete di Istituto e alla piattaforma è concesso soltanto se l'utilizzatore:

a) È stato prima di tutto identificato ovvero sono conosciute le sue generalità ed è stato dotato di credenziali utente (nome utente, password e/o PIN) soggette alle condizioni previste;
b) Effettua l'autenticazione tramite immissione delle credenziali, in modo che la piattaforma possa verificare se l'individuo è realmente chi sostiene di essere;
c) È stato autorizzato ovvero gli è stato conferito il diritto ad accedere a specifiche risorse in base al ruolo ricoperto, al profilo e alle specifiche mansioni assegnate.

È da ricordare che sussiste in capo al soggetto titolare dell'account qualsiasi responsabilità delle azioni effettuate nell'utilizzo del collegamento "nome utente e password e/o PIN", a meno di comprovato illecito da parte di terzi.

Gli account di accesso hanno, per impostazione predefinita, una scadenza corrispondente alla data di fine del contratto, estendibile su specifica autorizzazione del Dirigente scolastico.

Il personale con funzione di Amministratore della piattaforma è specificatamente autorizzato a gestire gli account utente per tutto il ciclo di vita tramite apposita procedura (creazione, aggiornamento, nuovi profili di autorizzazione, reset della password, disattivazione una volta concluso il rapporto di lavoro).

La normativa vigente in tema di protezione dei dati, le norme volontarie e le best practice di settore impongono di stratificare le possibilità di accesso ai contenuti e alle applicazioni presenti in piattaforma in modo da garantire un adeguato livello di sicurezza. Ad ogni account utente è collegato uno specifico profilo di autorizzazione che permette al singolo utilizzatore l'accesso in funzione del proprio ruolo, delle attività a cui è delegato e specificatamente autorizzato; eventuali estensioni o eccezioni devono essere autorizzate e tracciate secondo procedura.

Il sistema di Autenticazione, Autorizzazione e Registrazione degli accessi ha l'obiettivo di garantire un adeguato livello di sicurezza, conforme a quanto previsto dalla normativa vigente, poiché traccia, separa gli accessi nei livelli previsti, tutelando la riservatezza e l'integrità delle informazioni trattate.

Credenziali di autenticazione

Le credenziali di autenticazione sono composte da un codice (account utente) facilmente riconducibile al soggetto e da una password conosciuta dal solo utilizzatore. È tassativamente vietato rivelare le proprie credenziali di accesso alla piattaforma. Qualsiasi azione effettuata utilizzando la coppia "account utente e password" sarà attribuita in termini di responsabilità all'utente titolare registrato, a meno di comprovato illecito da parte di terzi.

La lunghezza minima della password deve essere di almeno 8 caratteri; considerato che i sistemi di violazione impiegano tempistiche esponenzialmente proporzionali con la lunghezza della password da violare, è necessario considerare almeno 14 caratteri per gli account dei servizi on-line (es. posta elettronica, piattaforme web) e per gli account qualificati come Amministratori di sistema.

Le password non devono essere trascritte; per questo è importante che siano facili da ricordare. È consigliabile utilizzare tecniche di memorizzazione (es. Mi_P1@c3_l4_P1zz@).

È fondamentale utilizzare password diverse per scopi, piattaforme o applicativi diversi. L'eventuale violazione di un sistema potrebbe comportare effetti indesiderati su tutti gli altri sistemi, anche personali, riconducibili al medesimo soggetto.

Le password devono essere modificate ad intervalli regolari per ridurre l'eventuale finestra temporale di esposizione e comunque con cadenza di almeno 3 mesi (c.d. Password aging).

Le password non devono mai far riferimento a termini di senso compiuto poiché già contenute nei dizionari utilizzati dai sistemi di violazione e neppure essere troppo ovvie (es. 'P@ssword').

Le password non devono essere in alcun modo collegate alla vita privata o lavorativa dell'utilizzatore. Sono quindi da escludere i nominativi dei familiari, la data di nascita, il codice identificativo, la targa dell'auto, la squadra del cuore, il soprannome, ecc. (elenco non esaustivo).

Le password devono contenere combinazioni di caratteri Maiuscoli, minuscoli, numeri e caratteri speciali (!, £, $, %, &, /, =, ?, §, @, #, …) anche quando non specificatamente richiesto dal sistema utilizzato (criteri di complessità).

Le password non devono essere riutilizzate a breve distanza di tempo; la rotazione minima prevista è almeno pari a 5 password diverse consecutive (c.d. Password history).

Le credenziali di accesso non devono essere comunicate a nessuno, per nessun motivo, con nessun mezzo. In caso di problemi di accesso alle risorse, è opportuno far riferimento al supporto tecnico o all'amministratore della piattaforma.

La digitazione delle password deve avvenire in massima sicurezza evitando di mostrare a terzi la sequenza dei tasti premuti. I colleghi impegnati in attività condivise al computer sono tenuti a voltarsi nel caso sia richiesta l'autenticazione al sistema o alla piattaforma software utilizzati.

La memorizzazione delle password nei browser è vietata a meno di attivazione di meccanismi di messa in sicurezza. Ad esempio, nel caso si utilizzi Mozilla Firefox è possibile attivare la funzione 'Utilizza una password principale' inserendo una password estremamente complessa e lunga.

Non utilizzare strumenti web per la generazione o il controllo del livello di sicurezza (utilizzare eventualmente password con costruzione simile al solo fine di verificarne la robustezza; es. https://password.kaspersky.com/it).

Per l'invio delle password di criptazione dei file e della documentazione non utilizzare mai lo stesso canale (es. file criptato inviato via posta elettronica e password comunicata a voce, via telefono).

Non seguire le tendenze del momento, non utilizzare acronimi, pattern ('CristianoRonaldo$' oppure sempre il primo carattere di ogni parola maiuscolo e un dollaro finale), ripetizioni e sequenze ('11111Paperin0000' oppure 'QWERTY12345') o parole presenti nei dizionari delle password più utilizzabili (reperibili in Internet).

Nel caso di perdita (o anche solo il sospetto di perdita) della segretezza della password è necessario:

a) Modificare immediatamente la password in uso
b) Comunicare l'accaduto all'Amministratore di Sistema e al Dirigente Scolastico che provvederà ad informare il DPO (Responsabile per la Protezione dei Dati) per la valutazione della gravità della situazione e l'attivazione delle procedure di emergenza in caso di incidente alla sicurezza, al fine di attivare tutti i controlli e le contromisure specifiche.

Nel caso l'utilizzatore sbagli per più di 5 volte l'inserimento della password, l'account viene automaticamente disabilitato; per effettuare la riabilitazione dell'account è necessario contattare l'Amministratore di Sistema o, se presente, utilizzare il sistema di *self-service password*.

Nei casi di particolare emergenza oppure in presenza di comportamenti che possano comportare problemi di sicurezza, l'Amministratore di Sistema è autorizzato alla momentanea disattivazione dell'account e, se

possibile, del sistema utilizzato. Risolta la problematica evidenziata, sarà cura dell'Amministratore di Sistema ripristinare le precedenti autorizzazioni.

È tassativamente vietato memorizzare credenziali di accesso in documenti salvati in sistemi o dispositivi al di fuori del perimetro di Istituto e ad accesso pubblico, inclusi sistemi di file hosting (come Google Drive o Dropbox).

In caso di violazione delle norme stabilite dal regolamento adottato, l'Istituto nella persona del suo rappresentante legale, il Dirigente Scolastico, potrà sospendere l'account dell'utente o revocarlo in modo definitivo senza alcun preavviso e senza alcun addebito a suo carico e fatta salva ogni altra azione di rivalsa nei confronti dei responsabili di dette violazioni.

L'Amministratore di Sistema ha potenzialmente accesso a qualsiasi dato memorizzato all'interno degli account creati, inclusa la e-mail, ma può accedervi esclusivamente per la verifica del buon funzionamento del sistema o su specifica indicazione dell'Autorità Giudiziaria.

I docenti e gli studenti sono tenuti a comunicare all'Amministratore di Sistema (adminricci@iismatteoricci.edu.it) eventuali gravi anomalie del servizio, comunicare eventuali violazioni della privacy al Dirigente Scolastico e segnalare all'amministratore G Suite ed al Dirigente Scolastico eventuali usi impropri del servizio di cui si è giunti a conoscenza.

Pertanto, in caso di malfunzionamenti, anomalie o presunte violazioni del sistema, l'Amministratore della piattaforma G Suite verifica le attività in corso attraverso i log o i contenuti in forma aggregata riferibili agli account degli utenti, nel rispetto della vigente disciplina sulla protezione dei dati personali e in conformità a quanto previsto dal provvedimento dell'Autorità Garante sugli Amministratori di Sistema. Per ulteriori informazioni si rinvia al link: https://support.google.com/accounts/answer/181692?hl=it.

L'Istituto si riserva la facoltà di segnalare alle autorità competenti per gli opportuni accertamenti ed i provvedimenti del caso, le eventuali violazioni alle condizioni di utilizzo indicate nel presente Regolamento, oltre che alle leggi ed ai regolamenti vigenti.

Dovranno essere adottate procedure dirette a revocare l'account dopo 30 giorni dal termine del percorso di studi presso l'Istituto per gli studenti e del rapporto lavorativo per i docenti assunti a tempo indeterminato e determinato (con termine incarico: 30 giugno). Nel caso di supplenze brevi, l'account sarà revocato dopo 15 giorni dal termine del contratto. Pertanto, i suddetti utenti dovranno provvedere a scaricare e salvare dal proprio account i materiali e i file di interesse in tempo utile poiché trascorso tale periodo gli stessi contenuti saranno irrimediabilmente cancellati.

L'Istituto si impegna a tutelare i dati forniti dall'utente in applicazione del Regolamento (UE) 2016/679 e del D.lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) e successive modifiche e integrazioni, ai soli fini della creazione e mantenimento dell'account.

Il servizio G-Suite è erogato da Google Inc. che applica una propria politica alla gestione della privacy; l'utente può conoscere in dettaglio il contenuto della policy visitando il sito web del fornitore al seguente link: https://www.google.com/intl/it/policies/privacy/.

Registrazione delle attività (Accounting)

A partire dall'accesso ai sistemi o ai dispositivi, le attività degli utilizzatori sono registrate in appositi file detti *log* che contengono informazioni come denominazione dell'utente, indirizzo IP o nome macchina, ora, data e dettaglio delle azioni svolte.

Al fine di contenere lo spazio necessario alla conservazione, i file di log sono conservati in logica di rotazione, ovvero sono sovrascritti al raggiungimento di una certa data o di una certa dimensione. Alcuni file di log (es. log di accesso) sono conservati nei sistemi per un periodo di almeno 2 anni dall'evento.

Tipologia di dati trattati rispetto alle finalità previste

Qualsiasi informazione riconducibile ad un soggetto, come un numero di matricola, un codice fiscale, un numero di telefono o una e-mail, è un dato personale subordinato alle regole previste dalla normativa vigente.

Solitamente gli esercizi didattici pubblicati in piattaforma non contengono dati personali, a meno dell'eventuale nome del docente o nomi degli allievi nelle consegne, con un'esposizione ai rischi molto limitata nei confronti degli interessati.

Dal punto di vista della conformità alla dottrina sulla protezione dei dati personali, i contenuti dei documenti relativi ai soggetti più fragili o contenenti dati personali di tipo particolare non dovrebbero essere caricati né condivisi in piattaforma poiché al di fuori del perimetro delle previste finalità, a meno che non siano adottate specifiche tecniche di pseudonimizzazione o di criptazione.

La semplice sostituzione del nome con la matricola del soggetto può essere senz'altro considerato un elemento sufficiente di sicurezza, avendo però cura di non rendere reperibile la decodifica all'interno dello stesso contenitore.

L'altra tecnica di sicurezza, ovvero la criptazione con password dei documenti dai contenuti riservati, è già disponibile nei pacchetti di produttività individuale (come ad es. MS-Office) o integrabile tramite strumenti esterni (es. 7zip). Unico vincolo da tener presente è la condivisione della chiave di criptazione o delle regole di costruzione della chiave stessa, in modo da risultare facile da ricordare per tutti i soggetti autorizzati senza bisogno di continui contatti o comunicazioni.

Tecniche di protezione (modalità condivisione e invio)

Le operazioni eseguite con gli strumenti informatici potevano un tempo risultare molto complesse; oggi le attuali piattaforme web risultano al contrario semplici e alla portata di tutti, disponibili su tutti i dispositivi. Quest'attività da un lato ha favorito il processo di digitalizzazione dei processi ma dall'altro, senza le dovute attenzioni, espone tutti gli operatori e gli interessati ai rischi legati alla condivisione. I danni prodotti dalla condivisione globale di una cartella riservata potrebbero risultare estremamente rilevanti, in termini risarcitori come sanzionatori.

Le condivisioni devono essere impostate a livello di amministrazione della piattaforma e verificate periodicamente, evitando il continuo scambio di link di accesso ai file e alle cartelle online tra soggetti altrimenti non autorizzati.

Nel caso di invio tramite posta elettronica di informazioni riservate, particolari o relative a soggetti sottoposti a maggior tutela, è necessario prevedere l'adozione delle tecniche sopra indicate ovvero la pseudonimizzazione e la criptazione. L'invio di documentazione ufficiale avente valore giuridico dovrebbe avvenire solamente attraverso i canali ufficiali (protocollo e PEC).

L'invio di documenti anche fotografati attraverso WhatsApp o altri prodotti di *instant messaging* non è ammesso. Sono invece accettabili i gruppi di condivisione per il solo scambio di informazioni di servizio, senza riferimenti di nessun tipo a fatti o a persone poiché la criptazione end-to-end garantita da queste piattaforme non è in realtà un elemento sufficiente di tutela.

Tempistiche di conservazione

I materiali, le cartelle, la posta elettronica del personale docente è conservata per ulteriori 30 giorni dopo la scadenza del contratto. Trascorso tale termine tutti i contenuti sono cancellati definitivamente senza produrre copie di backup e quindi senza nessuna possibilità di recupero.

Alla conclusione di un ciclo scolastico i contenuti riferibili ad una classe e ai singoli allievi sono eliminati definitivamente senza produrre copie di backup e dunque, anche in questo caso, senza nessuna possibilità di recupero.

I contenuti presenti in piattaforma, nelle aree ad accesso ristretto dei docenti in servizio continuativo nello stesso Istituto, sono sottoposti alle stesse regole sopra esposte.

Rimane in capo al singolo docente procedere periodicamente alla cancellazione dei dati riferibili a trattamenti di dati personali dalle finalità concluse e dei quali non è richiesta la conservazione.

Dispositivi utilizzati (BYOD), a scuola e a casa

I dispositivi di proprietà personale, anche detti BYOD (Bring Your Own Device, letteralmente "porta il tuo dispositivo"), possono essere utilizzati in Istituto per il collegamento ad Internet (Wi-Fi con accesso di tipo *guest*) ma NON direttamente collegati alla rete locale (ad esempio tramite cavo di rete LAN).

I soggetti che effettueranno collegamenti di tipo diretto alla rete LAN di Istituto (ad esclusione dei Wi-Fi pubblici) saranno sottoposti a sanzioni disciplinari; inoltre potranno essere addebitati loro eventuali costi di ripristino o ulteriori danni che dovessero originarsi dal collegamento non autorizzato.

Il collegamento alla rete Wi-Fi di Istituto dei dispositivi di proprietà personale come laptop, tablet o smartphone è possibile seguendo la specifica procedura di autorizzazione, registrazione e autenticazione.

In conformità alla normativa vigente in tema di protezione dei dati personali, è vietato salvare sui BYOD i dati personali, specialmente se di natura particolare, acquisiti o raccolti durante lo svolgimento delle attività lavorative a meno dell'adozione di tecniche di anonimizzazione, pseudonimizzazione o criptazione.

I personal computer personali posizionati presso il proprio domicilio non dovrebbero essere utilizzati per conservare documenti contenenti dati personali degli allievi né tantomeno informazioni sensibili o riservate, specie nel caso di utilizzo condiviso dei sistemi o dei dispositivi con familiari o altri soggetti.

Il trasporto al di fuori del perimetro aziendale di dispositivi di memorizzazione personali contenenti dati sensibili non protetti è vietato. Eventuali repliche o copie di sicurezza delle informazioni devono essere autorizzate e tracciate secondo le procedure previste. La responsabilità in caso di perdita, smarrimento e involontaria diffusione dei dati contenuti nel dispositivo, durante il trasporto al di fuori dall'Istituto, sarà attribuita all'utilizzatore registrato.

Nella malaugurata ipotesi di smarrimento o furto di un dispositivo BYOD contenente dati personali riconducibili all'Istituto titolare del trattamento dei dati, è obbligatorio comunicare l'accaduto al DPO/RPD per l'attivazione della procedura di *data breach*.

Ulteriori elementi di sicurezza delle sessioni

Sfortunatamente durante la fase di lockdown sono state numerose le segnalazioni di accessi abusivi alle sessioni online subite da molteplici istituti scolastici; questi attacchi non sono stati effettuati da hacker esperti ma causati principalmente dalla scarsa conoscenza degli strumenti o da inadeguate impostazioni di sicurezza.

Data l'elevata frequenza di queste incresciose situazioni, i fornitori delle piattaforme sono corsi ai ripari prevedendo e integrando specifiche limitazioni di sicurezza, da attivare preliminarmente o al momento dell'inizio della sessione.

A livello scolastico sono già attive le seguenti funzionalità di sicurezza:

1. Accettazione dei partecipanti alla sessione soltanto dal *dominio di appartenenza* dell'Istituto, creato al momento dell'attivazione della G-Suite (*Approve requests to join*);
2. Condivisione della sessione tramite agenda comune o meglio tramite *nickname* della sessione, in modo che la stessa non risulti riutilizzabile;
3. Moderazione gestita soltanto dal docente, unico soggetto in grado di disattivare o attivare i microfoni altrui, di consentire la condivisione dello schermo, di rimuovere i disturbatori dalle chat o ammettere nuovi partecipanti;
4. Sala di aspetto o *waiting room* con approvazione manuale degli invitati (al momento dell'inizio della lezione l'insegnante ammette soltanto coloro che appartengono alla classe);
5. "Stanza virtuale" chiusa a chiave, anche tramite un PIN;
6. Estromissione o modalità *mute* nei confronti dei soggetti che arrecano disturbo;
7. Attivazione di strumenti specifici verticalizzati sulla piattaforma, prodotti da terze parti;
8. Disabilitazione della connessione tramite telefono (solo audio) alla conferenza.

Pur in condizioni di emergenza non è mai auspicabile la condivisione dei link alle sessioni sui *social network* o sui sistemi di *instant messaging* in quanto è necessario evitare l'accesso a queste piattaforme da parte di estranei o semplicemente degli amici degli allievi "burloni".

In tal caso è possibile segnalare l'accaduto a Google al seguente indirizzo:

https://support.google.com/meet/contact/abuse?authuser=0&hl=it

Nei casi più gravi è necessario informare il Dirigente Scolastico e il DPO/RPD per effettuare la registrazione di violazione, seppure limitata, nell'apposito registro ed in seguito valutare l'eventuale necessità di segnalazione alla Polizia Postale.

Mappa dati – accessi

Di seguito è riportata una mappa con i destinatari (*audience*) che hanno la possibilità di visionare diverse tipologie di dati personali e quali dati personali sono utilizzati all'interno della piattaforma:

Audience / Dati personali	Studenti	Insegnanti	Amministratori di Sistema
Nominativo	✓	✓	✓
Nome utente	✓	✓	✓
Data di nascita	✘	✘	✓
Classe	**Soltanto la propria**	**Soltanto le assegnate**	✓
Valutazioni	**Soltanto le proprie**	**Soltanto le classi assegnate**	✓
e-mail	✓	✓	✓
File personali	**Solo i condivisi**	**Solo i condivisi**	✓
Riprese in conference	✓	✓	✓

In caso di condivisione all'esterno dei documenti, sono visibili anche le seguenti informazioni:

Dato personale	Visibilità rispetto ad una condivisione esterna
Nominativo	✓
Nome utente	✓
e-mail	✓

Componenti della suite utilizzati

Denominazione	Descrizione
Gmail	sistema di posta elettronica per l'invio di e-mail intra corso e verso il mondo Internet
Drive	è il servizio di file hosting o cloud storage personale in cui gli utenti possono archiviare dati e sincronizzare i loro contenuti sui diversi dispositivi. I contenuti possono essere condivisi con altri utenti della suite e non solo
Calendar	Gestione calendario e condivisione degli appuntamenti
Documenti, Fogli e Presentazioni	Sistema di produttività individuale per lavorare su documenti, fogli di lavoro e presentazioni.
Moduli	Gestione Moduli, quiz e sondaggi per raccogliere le risposte e analizzarle con l'aiuto del sistema di *machine learning*
Jamboard	a lavagna smart disponibile su computer, telefono o tablet
Sites	strumento per la realizzazione di siti web, programmi di studio, sviluppo di competenze e al fine di dare sfogo alla creatività degli studenti.
Meet	videochiamate e messaggi per la Didattica a distanza
Gruppi	Forum di classe
Vault	Controllo e monitoraggio delle impostazioni di sicurezza dei dispositivi
Classroom	Gestioni assegnazioni, compiti e feedback

Riferimenti normativi

- Regolamento (UE) 2016/679
- D.lgs. 196/2003 novellato D.lgs. 101/2018
- Provvedimento Autorità Garante del 26 marzo 2020 - "Didattica a distanza: prime indicazioni" [Doc. web n. 9300784] https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9300784
- Circolare AgID n. 3 del 9 aprile 2018
- Piano Triennale per l'informatica della PA (AgID)

Sitografia

Marketplace AgID https://cloud.italia.it/marketplace

Google Suite https://edu.google.it

MIUR DaD https://www.istruzione.it/coronavirus/didattica-a-distanza_google-education.html