UNIONE EUROPEA
FONDI STRUTTURALI EUROPEI
PON 2014-2020
MIUR
Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
Direzione Generale per interventi in materia di edilizia scolastica, per la gestione dei fondi strutturali per l'istruzione e per l'innovazione digitale
Ufficio IV
PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO (FSE-FESR)

Istituto Comprensivo Statale "Alto Casertano"
Istruzione del primo ciclo nei comuni di
ROCCAMONFINA-ROCCAD'EVANDRO-CONCA DELLA CAMPANIA-GALLUCCIO-SAN PIETRO INFINE-TORA E PICCILLI
Via S. Lucia - 81035 - ROCCAMONFINA (CE) - Tel. 0823/677280
ceic8be00b@istruzione.it ♦ ceic8be00b@pec.istruzione.it ♦ http://www.icaltocasertano.it
Codice meccanografico CEIC8BE00B ♦ Codice Fiscale 95022400618

Roccamonfina, lì 13/06/2023

COMUNICAZIONE N.193

A tutti i docenti

Al personale ATA

Al D.S.G.A.

Albo

Sito web

Gentile Docente, Personale ATA e DGSA,

l'uso delle piattaforme all'interno degli istituti scolastici ha avuto un'accelerazione notevole a seguito dell'emergenza Covid19. Sempre più spesso se ne è appreso l'utilità e l'indispensabilità, ma alcune volte la facilità d'uso e la possibilità di fare nuove attività in modalità digitale, che prima si potevano svolgere solo in modalità analogica, hanno fatto trascurare la sicurezza dei dati e la privacy.

Nella platea dei docenti e ATA sono aumentate le competenze digitali e si sono aperti nuovi scenari, ma ora è necessario riportare l'uso della tecnologia in conformità alle normative vigenti.

È il caso di ricordare la definizione di dato personale: "**informazioni che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica**" quindi anche semplicemente ***nome e cognome***. Inoltre ricordiamo la definizione di dato particolare (ex sensibile): **quei dati personali che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale,** ai quali oggi possiamo aggiungere, in alcuni casi la mail, il numero di telefono, l'indirizzo IP, il MAC Address (un numero di identificazione univoco che ti aiuta a rintracciare il tuo dispositivo in una rete).

Ogni qualvolta trattiamo queste informazioni in modalità analogica (carta, voce, ecc.) o in modalità digitale (piattaforme, mail, ecc.) stiamo effettuando un **trattamento dati** e pertanto siamo soggetti alla privacy GDPR 679/2016 e Dlgs 196/2003.

Quando trattiamo dati dobbiamo rispettare tutte le misure di sicurezza prescritte. Tra queste vogliamo dare evidenza in particolare a due: **Nomina a Responsabile Esterno del Trattamento Dati** e **Divieto di Trasferimento Dati Extra UE** (in realtà SEE Spazio Economico Europeo).
Un serie di accordi per trasferire dati di cittadini europei negli Stati Uniti, è stato fatto decadere attraverso la sentenza "Schrems II" del 27/04/21 della Corte di Giustizia Europea (vedi anche Privacy Shield), ponendo il divieto al trasferimento dei dati. La sentenza è fortemente limitante verso il trasferimento negli USA. Non basta che i dati siano in Europa considerato che le società statunitensi sottostanno a controlli che consentono di acquisire informazioni anche in altri paesi (vedi potere della CIA ed FBI).

Nell'aprile 2021 (sentenza Schrems II) eravamo in pandemia e c'era lo stato di emergenza, quindi di fronte alla situazione questo divieto è stato disatteso. Ora che non siamo più in emergenza alcune "cattive abitudini" sul trattamento dati non sono più tollerabili. Ci vediamo costretti ad intervenire sulla questione, solo così possiamo garantire la necessaria sicurezza dati senza incorrere in eventi lesivi della privacy.

Piattaforme come Google Workspace (ex G-Suite), Microsoft Office 365 / Teams ed altre possiamo continuare ad utilizzarle se attuiamo stringenti misure di sicurezza ed evitiamo di effettuare trattamenti dati non strettamente necessari e non legati strettamente ad attività didattiche e formative. In alternativa dovremo smettere di utilizzarle.

Quale sono le azioni che potremo mettere in atto per aumentare la sicurezza:

- Pseudonimizzare gli account (non più nome.cognome@dominio.edu.it)
- Utilizzare solo finestre di navigazione in incognito quando si usano le piattaforme;
- Usare sistemi di VPN in modo da mascherare indirizzo IP ed altre informazioni personali;
- non usare Forms (moduli) per attività diverse dalla didattica (es. no uso per censire scioperanti)
- non usare Google Drive o OneDrive per condividere PEI, PDP, altri documenti riportanti dati personali, foto, video;
- non usare YouTube per pubblicare video di alunni;
- non usare Facebook, Instagram, ed altre piattaforme per condividere foto e video;
- non usare Canva per stampare locandine e attestati con nominativi di alunni/docenti;
- non usare WhatsApp per condividere documenti, foto e video di alunni;
- non utilizzare piattaforme tipo "I love PDF" per manipolare PDF contenenti dati;
- non utilizzare alcuna piattaforma non ufficiale dell'istituto per gestire dati personali, foto e video di alunni.

Questi ovviamente sono degli esempi non esaustivi che danno le opportune indicazioni.

Con questo non vogliamo limitare la tecnologia, ma solo farne un uso consapevole ricordando che **SIAMO SOGGETTI A QUESTE REGOLE SOLO SE TRATTIAMO DATI PERSONALI**.

La strategia per fare tutto ciò a cui ci siamo abituati è quella di pseudonimizzare. Esempio pratico: **ho alunni per cui ho redatto i PEI**? Inserendo al posto del nome e cognome gli pseudonimi tipo Pippo, Pluto e Paperino, non ho inserito dati personali che possano consentire ai non titolati di identificare le persone fisiche, quindi posso salvarli su Google Drive e condividerli con Whatsapp.
L'attenzione su queste questioni è stata sollecitata anche dal Ministero dell'Istruzione e del Merito nella circolare n. 706 del 20/03/2023 con allegati Approfondimenti tecnici di supporto per le istituzioni scolastiche.
Anche il nostro DPO ha fornito indicazioni tecniche e suggerimenti per continuare a utilizzare le attuali piattaforme mitigando il rischio (purtroppo non c'è modo di azzerarlo), ovvero sospenderle in caso di mancata attuazione di misure tecniche idonee.
Considerata la situazione transitoria in attesa dell'emanazione di un nuovo Privacy Shield, la responsabilità esclusiva verso terzi del Dirigente scolastico, la non stretta necessità dell'uso di queste piattaforme decaduto lo stato di emergenza, la necessità di riportare le stesse piattaforme ad un uso prettamente didattico e non anche amministrativo, la possibilità nel nuovo anno scolastico di continuare ad usare le attuali piattaforme con l'attuazione di misure più stringenti, ovvero l'attivazione di nuove piattaforme, tenuto conto anche dei fondi PNRR,

IL DIRIGENTE SCOLASTICO

- consente l'uso della piattaforma Google Workspace / Microsoft Office 365 subordinato all'applicazione delle seguenti misure di sicurezza tecniche MT e comportamentali MC:
    - MT - Blocco del sistema di posta elettronica in piattaforma Google/Microsoft;
    - MT - Chiusura della posta elettronica Google/Microsoft da e verso l'esterno;
    - MT - Attuazione della pseudonimizzazione dei nominativi e degli indirizzi mail della piattaforma;

- MT – Attuazione di sistemi di cifratura negli scambi dati in piattaforma (solo su piattaforme a pagamento che lo consentono;
- MT – Acquisto di versione superiore della piattaforma che consente la localizzazione dei dati nello Spazio Economico Europeo;
- MT – Altre misure tecniche oggettive scelte dalla scuola / amministratore piattaforma (descrivere nel dettaglio);
- MT – Uso esclusivo di dispositivi della scuola, dotati di misure di protezioni sui dati, che periodicamente vengono resettati;
- MC – Non uso di dati personali / particolari in nessuna sezione / App della piattaforma;
- MC – Utilizzo di finestre di navigazione in incognito;
- MC – Utilizzo di browser diverso dal produttore della piattaforma, ovvero utilizzo di browser più efficaci nello nel mascherare l'utente;
- MC – Utilizzo di sistemi di VPN;

- invita i docenti ad effettuare copia dei dati presenti in Drive, Classroom, Forms, Mail e altre applicazioni connesse (in genere tutti i contenuti sono allocati in Google Drive o Microsoft OneDrive);
- invita tutto il personale docente e non docente ad un utilizzo consapevole e responsabile, in ambito scolastico, di tutte quelle app e quei software e servizi cloud, non autorizzati dalla scuola o provenienti da fonti sconosciute e di accertarsi che i file in transito in essi non siano conservati in server non europei e comunque che non siano di aziende di origine statunitense o per le quali non vi è un accordo sulla trasferibilità dei dati al di fuori dello SEE o comunque non compatibili con GDPR 679/2016;
- invita ad aggiornare l'indirizzo di posta nelle varie registrazioni effettuate con l'indirizzo di posta nome.cognome@posta.istruzione.it , indirizzo ufficiale per le attività lavorative fornito e garantito dal MIM;
- invita a riattivare, qualora fosse sospeso o fosse stata smarrita la password, l'indirizzo di posta nome.cognome@posta.istruzione.it in autonomia accedendo ad Istanze OnLine https://www.istruzione.it/polis/Istanzeonline.htm con proprio SPID, operazione semplice da compiere;
- prescrive di RIMUOVERE tutti i dati personali/particolari salvati in piattaforma;
- prescrive di evitare, anche nelle comunicazioni, l'uso di dati personali e particolari quando non è strettamente necessario ed indispensabile;
- prescrive fare massima attenzione a qualsiasi trattamento dati e comunicazione effettuata.

Si ricorda, inoltre, che la piattaforma di Registro elettronico non è soggetta a queste criticità e quindi può essere utilizzata con tranquillità, ma sempre nel rispetto di GDPR che prescrive il non utilizzo di dati personali qualora non sia strettamente necessario.

Per quanto riguarda le videoconferenze sono sospese, ovvero sono consentibili previo richiesta esplicita da parte delle persone adulte interessate.

Considerata la particolarità della tematica in oggetto, si confida in un'attenta osservazione delle indicazioni da parte di tutto il personale.

IL DIRIGENTE SCOLASTICO
Prof.ssa Reginia Assunta di Zazzo
Documento firmato digitalmente ai sensi del Codice dell'Amministrazione Digitale e normativa connessa