LICEO STATALE "G. FRACASTORO"
Via G.B. Moschini,11/A; tel. 045 8348772; fax 045 8343626;
Sito web: www.liceofracastoro.edu.it - Email vrps03000r@istruzione.it
VERONA

PROT. IN SEGNATURA ALLEGATA

REGOLAMENTO FINALIZZATO ALLA MITIGAZIONE DEI RISCHI DERIVANTI DALL'USO DELLA PIATTAFORMA GOOGLE

CONSIDERATO che l'utilizzo della Piattaforma Google, per fronteggiare la pandemia da Sars Cov2, è stato consigliato dal MIUR (ora MIM) mediante pubblicazione sul Sito Ufficiale del Ministero;

CONSIDERATO che il Garante, con provvedimento n. 64 del 26 marzo 2023, intitolato *Didattica a distanza: prime indicazioni*, ha riconosciuto una specifica base giuridica all'utilizzo delle piattaforme digitali, affermando che «le scuole e le università sono autorizzate a trattare i dati, anche relativi a categorie particolari, di insegnanti, alunni (anche minorenni), genitori e studenti, funzionali all'attività didattica e formativa in ambito scolastico, professionale, superiore o universitario (art. 6, parr. 1, lett. e), 3, lett. b) e 9, par. 2, lett. g) del Regolamento e artt. 2-ter e 2-sexies del Codice)»;

ACCERTATO che il Garante, nel provvedimento n. 64 del 26 marzo 2023, intitolato *Didattica a distanza: prime indicazioni*, ha dichiarato che «non deve pertanto essere richiesto agli interessati (docenti, alunni, studenti, genitori) uno specifico consenso al trattamento dei propri dati personali funzionali allo svolgimento»;

ACCERTATO che il Garante, nel provvedimento n. 64 del 26 marzo 2023, intitolato *Didattica a distanza: prime indicazioni*, ha stabilito che «la valutazione di impatto, che l'art. 35 del Regolamento richiede per i casi di rischi elevati, non è necessaria se il trattamento effettuato dalle istituzioni scolastiche e universitarie, ancorché relativo a soggetti in condizioni peculiari quali minorenni e lavoratori, non presenta ulteriori caratteristiche suscettibili di aggravarne i rischi per i diritti e le libertà degli interessati. Ad esempio, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola (non, quindi, su larga scala) nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consente il monitoraggio sistematico degli utenti o comunque non ricorre a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici)»;

CONSIDERATO che, per l'utilizzo delle Piattaforme digitali, il Liceo Statale G. Fracastoro, in qualità di titolare del trattamento, è tenuto a valutare l'adozione di misure per rafforzare la piena conformità al GDPR, come previsto dal Provvedimento del Garante n. 64 del 26 marzo 2020;

CONSIDERATO che il Garante, nel Provvedimento n. 64 del 26 marzo 2020, si è in ogni caso impegnato a valutare «l'opportunità di avviare verifiche sui fornitori delle principali piattaforme per la didattica a distanza per assicurare il rispetto del Regolamento e del Codice in relazione ai trattamenti effettuati per conto delle scuole»;

ACCERTATO che al momento non si registrano comunicazioni del Garante che segnalino alle Istituzioni Scolastiche impedimenti all'uso della piattaforma Google, attualmente in uso presso il Liceo Statale G. Fracastoro;

CONSIDERATO che, per l'utilizzo delle Piattaforme digitali, il Liceo Statale G. Fracastoro, in qualità di titolare del trattamento, ha proceduto a valutare l'opportunità delle verifiche sulle piattaforme digitali utilizzate dall'Istituto;

CONSIDERATO il principio di responsabilizzazione;

CONSIDERATO che la piattaforma Google può essere considerata sicura rispetto al rischio di cyber attacchi;

CONSIDERATE le necessità istituzionali che mettono capo alle Istituzioni Scolastiche, con particolare riferimento alle finalità:

a) didattiche, poiché la digitalizzazione della didattica e degli ambienti di apprendimento costituiscono elementi imprescindibili del PNRR, ed in particolare del Piano Scuola 4.0, che obbliga le Istituzioni Scolastiche a procedere nel senso dell'innovazione degli ambienti di apprendimento e dello sviluppo di una didattica innovativa, che assuma ed utilizzi i nuovi strumenti digitali e le piattaforme che ne consentono l'utilizzo;
b) amministrative, come per altro dimostrato dall'adozione del PON *Digital Board: trasformazione digitale nella didattica e nell'organizzazione Fondi Strutturali Europei – Programma Operativo Nazionale "Per la scuola, competenze e ambienti per l'apprendimento" 2014-2020. Asse II - Infrastrutture per l'istruzione – Fondo Europeo di Sviluppo Regionale (FESR) – REACT EU. Asse V – Priorità d'investimento: 13i – (FESR) "Promuovere il superamento degli effetti della crisi nel contesto della pandemia di COVID-19 e delle sue conseguenze sociali e preparare una ripresa verde, digitale e resiliente dell'economia" – Obiettivo specifico 13.1: Facilitare una ripresa verde, digitale e resiliente dell'economia - Azione 13.1.2 "Digital Board: trasformazione digitale nella didattica e nell'organizzazione"– Avviso pubblico prot.n. 28966 del 6 settembre 2021 per la trasformazione digitale nella didattica e nell'organizzazione*, realizzato dalla scrivente Istituzione scolastica;
c) organizzative, con evidenti ed ineludibili conseguenze sul piano propriamente organizzativo;

ACCERTATO che, per le ragioni esposte nel punto precedente, per il perseguimento delle proprie finalità istituzionali e dell'interesse pubblico le Istituzioni scolastiche necessitano dell'utilizzo degli strumenti digitali e delle piattaforme digitali;

VISTA la diffida del Collettivo MonitoraPA;

VISTO il Protocollo Euservice 2023 intitolato *Come gestire l'invio di dati in USA*, che individua espressamente tre opzioni, e cioè:

1. Abbandonare i sistemi americani;
2. Mantenere i sistemi americani senza alcun accorgimento;
3. Mantenere i sistemi usa, riducendo il rischio;

VISTO l'esito dell'Audit con il DPO del Liceo del giorno 21/04/2023;

VISTA, in particolare, l'ipotesi n. 3 del Protocollo Euservice 2023 intitolato *Come gestire l'invio di dati in USA*;

VISTE le misure individuate nell'Audit (svoltosi presso il Liceo Statale G. Fracastoro il giorno 21/04/2023 alla presenza del DPO, del Dirigente scolastico, della DSGA, dell'Animatore digitale, dell'AT per l'informatica, prot. 4338/2023) finalizzate alla graduale mitigazione dei rischi derivanti dall'uso della piattaforma Google;

LICEO STATALE "G. FRACASTORO"
Via G.B. Moschini,11/A; tel. 045 8348772; fax 045 8343626;
Sito web: www.liceofracastoro.edu.it - Email vrps03000r@istruzione.it
VERONA

VISTA la richiesta di parere inoltrata al DPO dell'Istituto dal Liceo Statale G. Fracastoro;

VISTO il parere reso dal DPO dell'Istituto del giorno 4/05/2023, prot. n. 3857/2023;

VISTO che le misure per graduale mitigazione dei rischi che sono state indicate nel modo seguente:

1. richiedere un parere all'ufficio legale di EUservice se l'utilizzo dei servizi Google a pagamento risolverebbe i problemi relativi alla privacy;
2. abbandonare il trattamento PEI e PDP effettuato attraverso la piattaforma procedendo in via sostitutiva alla loro predisposizione in formato cartaceo e successiva procedura di digitalizzazione attraverso scannerizzazione a norma del documento che verrebbe solo successivamente firmato digitalmente dal Dirigente;
3. cifratura del *repository* degli elaborati degli studenti la cui implementazione sarà a cura animatore digitale;
4. mettere in atto da parte del personale un controllo dei dati archiviati in cloud al termine dell'anno scolastico con cancellazione dei dati archiviati non più utili in relazione alla finalità, con particolare riguardo alla cancellazione dei dati raccolti attraverso moduli;
5. verificare la fattibilità di comunicare sistematicamente i provvedimenti disciplinari/dati potenzialmente giudiziari attraverso il registro elettronico soprattutto per quanto riguarda i flussi in uscita dalla segreteria a personale della scuola;
6. impartire disposizioni in merito all'anonimizzazione o alla pseudonimizzazione delle comunicazioni di dati sensibili effettuate attraverso posta elettronica;

VISTA la TIA (TRANSFER IMPACT ASSESSMENT, prot. n. 4339/2023) predisposta da Euservice ed accolta dal Liceo Statale G. Fracastoro del giorno;

VISTE le Ulteriori considerazioni del DPO a seguito dell'audit del 21 aprile, che confermano l'adeguatezza, al momento, delle misure di mitigazione individuate nel corso della predetta Audit del 21 aprile 2023 (prot. n. 4407/2023 del 19/05/2023;

VISTA la comunicazione via mail del giorno 8 giugno 2023 del DPO, che ritiene il presente Regolamento «adeguato per garantire ed essere in grado di dimostrare di essere *compliant* al GDPR»;

VISTA la Delibera del Consiglio di Istituto n. 25/2023 del giorno 22 giugno 2023;

AL FINE di mitigare gradualmente i rischi derivanti dall'uso della piattaforma Google;

FERMA RESTANDO la necessità di procedere nel corso del tempo a progressive modifiche e integrazioni del presente Regolamento in ragione dell'evoluzione delle innovazioni tecnologiche, delle necessità che dovessero emergere e delle eventuali nuove ed ulteriori disposizioni delle Autorità competenti;

IL DIRIGENTE SCOLASTICO

ADOTTA

le presenti disposizioni, che costituiscono il **primo Regolamento finalizzato alla mitigazione dei rischi derivanti dall'uso della piattaforma Google**.

LICEO STATALE "G. FRACASTORO"
Via G.B. Moschini,11/A; tel. 045 8348772; fax 045 8343626;
Sito web: www.liceofracastoro.edu.it - Email vrps03000r@istruzione.it
VERONA

REGOLAMENTO FINALIZZATO ALLA MITIGAZIONE DEI RISCHI DERIVANTI DALL'USO DELLA PIATTAFORMA GOOGLE

Art. 1 – Piattaforma Google; limitazione dei servizi forniti dalla Piattaforma Google

Per il perseguimento delle finalità istituzionali indicate nella premessa del presente Regolamento, il Liceo G. Statale G. Fracastoro utilizza la piattaforma Google.

Al fine di mitigare i rischi e di adempiere ai propri compiti istituzionali vengono utilizzati unicamente i servizi della piattaforma Google espressamente indicati dal seguente elenco:

- Gmail;
- Calendar;
- Classroom;
- Compiti;
- Contatti;
- Drive;
- Moduli;
- Gruppi;
- Sites;
- Presentazioni;
- Chat;
- Meet;
- Vault;
- Sincronizzazione Chrome.

All'utilizzo di tali sevizi si applicano le misure di mitigazione dei rischi stabiliti negli articoli del presente Regolamento.

Il Liceo Statale G. Fracastoro rinuncia espressamente a tutti i servizi aggiuntivi, come ad esempio Maps e You Tube.

Art. 2 – Trattamento dei dati sensibili contenuti nei PEI

Il trattamento dei dati personali e sensibili degli studenti e delle studentesse contenuti nei **Piani Educativi Individualizzati (PEI) non deve mai avvenire per mezzo della piattaforma Google**, del servizio Drive o mediante posta elettronica, sia privata che istituzionale.

A far data dalla pubblicazione del presente Regolamento docenti e personale di segreteria e, in genere, personale ATA non devono mai:

- trattare o trasferire i dati personali e sensibili degli studenti e delle studentesse con PEI via mail;
- citare i o trasferire i nomi degli studenti o studentesse con PEI via mail;

- trattare o trasferite i dati personali e sensibili degli studenti e delle studentesse con PEI facendo uso del servizio Drive.

In occasione degli Esami di Stato, i docenti sono tenuti a consegnare i documenti che contengono dati di studenti e studentesse con PEI in via riservata e su supporto cartaceo ai Presidenti delle Commissioni degli Esami di Stato istituite presso il Liceo Statale G. Fracastoro.

I dati personali e sensibili degli studenti e delle studentesse contenuti nei **Piani Educativi Individualizzati (PEI) devono sempre essere trattati su supporto cartaceo**.

Il personale docente comunica e trasmette tali dati alla segreteria esclusivamente su supporto cartaceo, sia per gli studenti e le studentesse della sede centrale che della succursale di via Cà di Cozzi.

Il personale di segreteria inserisce tali dati nel fascicolo personale dell'alunno, **in busta riservata**. Tali dati vengono depositati e conservati negli appositi armadi della segreteria didattica del Liceo.

Nel caso di consegna su supporto cartaceo dei documenti sopra indicati, il personale di segreteria, acquisite le eventuali firme previste dalle disposizioni vigenti, procede alla successiva procedura di digitalizzazione attraverso scannerizzazione a norma delle vigenti disposizioni dei documenti medesimi. Non appena terminata la scannerizzazione, tali documenti vengono immediatamente riposti in busta riservata e conservati negli appositi armadi della segreteria didattica.

Tali documenti vengono successivamente firmati digitalmente dal Dirigente scolastico ed archiviati secondo le vigenti disposizioni.

In ogni caso, l'archiviazione viene effettuata al di fuori della piattaforma Google.

Art. 3 – Trattamento dei dati sensibili contenuti nei PDP o nei PFP

Il trattamento dei dati personali e sensibili degli studenti e delle studentesse contenuti nei **Piani Didattici Personalizzati** (PDP, per studenti BES o DSA) o dei **Piani Formativi Personalizzai** (**PFP**, per studenti atleti) non deve avvenire per mezzo della piattaforma Google, del servizio Drive o mediante posta elettronica, sia privata che istituzionale.

A far data dalla pubblicazione del presente regolamento, docenti e personale di segreteria non devono mai:

- trattare o trasferite i dati personali e sensibili degli studenti e delle studentesse con PDP o PFP via mail;
- citare o trasferire i nomi di tali studenti o studentesse con PDP o PFP via mail;
- trattare o trasferite i dati personali e sensibili degli studenti e delle studentesse con PDP o PFP facendo uso del servizio Drive.

In occasione degli Esami di Stato, i docenti sono tenuti a consegnare i documenti che contengono dati di studenti e studentesse con PDP in via riservata e su supporto cartaceo ai Presidenti delle Commissioni degli Esami di Stato istituite presso il Liceo Statale G. Fracastoro.

I dati personali e sensibili degli studenti e delle studentesse contenuti nei **PDP e nei PFP** devono sempre essere trattati su supporto cartaceo.

Il personale docente comunica e trasmette tali dati alla segreteria esclusivamente su supporto cartaceo. Il personale di segreteria inserisce tali dati nel fascicolo personale dell'alunno, in busta riservata.

Nel caso di consegna su supporto cartaceo dei documenti sopra indicati, il personale di segreteria, acquisite le eventuali firme previste dalle disposizioni vigenti, si occupa della successiva procedura di digitalizzazione attraverso scannerizzazione a norma delle vigenti disposizioni dei documenti. Tali documenti vengono successivamente firmati digitalmente dal Dirigente scolastico ed archiviati secondo le vigenti disposizioni.

Non appena terminata la scannerizzazione, tali documenti vengono immediatamente riposti in busta riservata e conservati negli appositi armadi della segreteria didattica.

In ogni caso, l'archiviazione viene effettuata al di fuori della piattaforma Google.

Art. 4 – Uso della funzione "Bacheca" – mail tra docenti e tra docenti e segreteria: disposizioni sull'uso dei nomi

Si adotta il principio generale secondo cui la comunicazione indirizzata dal personale della scuola ai genitori delle studentesse e degli studenti o ai tutori avviene mediante le funzioni del Registro elettronico, che costituisce un'area di accesso protetta e limitata.

Nel caso in cui ricorra la necessità di comunicare ufficialmente elenchi di studenti e studentesse che partecipano a specifiche attività approvate dagli Organi Collegiali (a mero titolo di esempio: viaggi, uscite, visite, gare), la comunicazione della Scuola ha luogo unicamente mediante la funzione bacheca della classe del Registro elettronico.

Di norma, nelle mail tra i docenti e tra docenti e segreteria deve essere evitata nella misura più ampia possibile l'indicazione dei singoli nomi e cognomi degli studenti e delle studentesse.

In ogni caso, nelle mail tra docenti e tra docenti e segreteria **non devono mai essere contenuti dati sensibili e dati sullo stato di salute degli studenti o delle studentesse**.

Tra il personale scolastico la comunicazione di dati sensibili, giudiziari, sulla salute e, in genere, particolari, non deve mai avere luogo via mail.

La comunicazione dai genitori alla scuola di dati sensibili, giudiziari, sulla salute e, in genere, particolari, ha luogo su supporto cartaceo.

La trasmissione alla segreteria delle denunce di infortunio degli studenti e delle studentesse non deve mai avvenire via mail. In questi casi la denuncia e l'eventuale ulteriore documentazione vengono depositate in segreteria su supporto cartaceo. La segreteria si occupa della successiva procedura di digitalizzazione attraverso scannerizzazione a norma delle vigenti disposizioni del documenti depositati. Tali documenti vengono successivamente firmati digitalmente dal Dirigente scolastico ed archiviati secondo le vigenti disposizioni.

Non appena terminata la scannerizzazione, tali documenti vengono immediatamente riposti in busta riservata e conservati negli appositi armadi della segreteria didattica.

I docenti e il personale di segreteria non devono mai chiedere **via mail** ai genitori degli studenti o delle studentesse dati sensibili e dati sulla salute.

Art. 5 – Dati archiviati in cloud – cancellazione

Concluso l'anno scolastico, i dati personali degli studenti e delle studentesse archiviati in cloud non sono più utili e necessari per le finalità istituzionali del Liceo Statale G. Fracastoro.

La procedura di archiviazione dei compiti e delle verifiche segue le prescrizioni nell'art. 7 del presente regolamento.

Al fine di mitigare i rischi derivanti dall'uso della piattaforma Google, si stabilisce il controllo e la cancellazione dei dati archiviati in cloud.

A tal fine si dispone che, al termine di ogni anno scolastico, abbia luogo la cancellazione di tutti i dati personali degli studenti o delle studentesse eventualmente archiviati in cloud, con particolare riguardo alla cancellazione dei dati raccolti attraverso moduli di Google.

A tale scopo, l'Animatore Digitale forma opportunamente il personale ATA di segreteria affinché all'inizio di ogni anno scolastico, entro il mese di settembre, tutti i dati degli studenti e delle studentesse archiviati in cloud nell'anno precedente siano cancellati.

La formazione del personale ATA di segreteria a cura dell'Animatore Digitale ha luogo nei primi giorni del mese di settembre 2023. In seguito alla formazione il personale ATA di segreteria provvede alla predetta cancellazione.

In caso di necessità, tale formazione viene replicata negli anni successivi.

Art. 6 – Comunicazione dei provvedimenti disciplinari e giudiziari

Entro il mese di dicembre 2023 il Liceo Statale G. Fracastoro verifica la possibilità di comunicare sistematicamente i provvedimenti disciplinari e i dati potenzialmente giudiziari attraverso le funzioni del Registro elettronico.

In caso di esito positivo della verifica prevista nel primo comma del presente articolo, si dispone che il trasferimento di tutti i provvedimenti disciplinari, sia degli studenti e delle studentesse sia del personale scolastico, avvenga unicamente mediante il Registro elettronico.

In caso di esito positivo della verifica prevista nel primo comma del presente articolo, vengono impartite al personale di segreteria specifiche disposizioni di dettaglio.

Art. 7 – Procedura di archiviazione dei compiti degli alunni svolti in modalità digitale – *Repository*

Al fine di evitare:

- i rischi derivanti da una possibile perdita dei dati;
- il trattamento dei voti degli studenti nel momento dell'archiviazione;
- che i docenti vedano gli elaborati dei colleghi;

si adotta la seguente procedura per l'archiviazione dei compiti e delle verifiche degli alunni svolti con mezzi elettronici:

a) ciascun docente al termine delle lezioni (entro il 30 giugno) di ciascun anno scolastico provvede ad archiviare le proprie classi virtuali di G Classroom nella cartella di Drive creata e condivisa dall'Animatore Digitale nominata (Nome_Cognome_anno del docente);
b) ciascun docente sposta nella cartella a lui dedicata la singola cartella delle classi virtuali dei vari corsi inizialmente archiviata solo nel Drive personale;
Per effettuare questa operazione ciascun docente deve accedere al proprio Drive→Classroom, selezionare tutte le cartelle relative alle classi virtuali dell'anno scolastico in corso e spostarle nella cartella dedicata all'archiviazione.
c) I dettagli della procedura sono messi a disposizione dei docenti mediante un video tutorial a cura dell'animatore dall'Animatore Digitale.

Terminata l'operazione, al fine di tutelare i dati degli studenti e delle studentesse, ogni anno l'Animatore digitale, avvalendosi di uno specifico software, procede alla cifratura della *Repository*.

Art. 8 – Mail degli alunni – eventuale pseudonimizzazione

Il Liceo Statale G. Fracastoro è proprietario degli indirizzi mail creati dal Liceo medesimo e messi a disposizione degli studenti e delle studentesse iscritti al Liceo e contrassegnati in questo modo: *@liceofracatsoro.edu.it.*

Una volta creato l'indirizzo mail, al primo accesso gli studenti e le studentesse iscritti al Liceo modificano la propria password.

L'indirizzo mail viene cancellato al momento in cui lo studente o la studentessa non risulta più iscritta al Liceo Statale G. Fracastoro.

Entro il mese di settembre del 2023 il Liceo verifica la possibilità e la fattibilità della creazione degli indirizzi mail istituzionali degli studenti e delle studentesse iscritte al Liceo mediante l'uso di pseudonimi (ad esempio, per mezzo: del codice SIDI; dell'indicazione della classe seguita dal numero progressivo dell'alunno negli elenchi di classe; di altro metodo che dovesse essere ritenuto più funzionale e altrettanto capace di mitigare i rischi mediante pseudonimizzazione).

In caso di esito positivo, il Liceo procede alla creazione degli indirizzi mail dei nuovi iscritti mediante l'uso dello pseudonimo.

Art.9 – *Data breach*

In caso di *Data breach* docenti e personale ATA sono tenuti a leggere, a conoscere e a seguire scrupolosamente la procedura prevista per il *Data breach*.

La procedura prevista per il *Data breach* è stata pubblicata con circolare n. 28 bis del 14 settembre 2022; in caso di necessità, viene aggiornata.

In allegato al presente Regolamento si mette a disposizione di tutto il perdonale scolastico la procedura al momento in vigore.

Eventuali successive modifiche ed integrazioni della procedura prevista per il *Data breach* vengono tempestivamente pubblicate e integrano il presente Regolamento immediatamente e a tutti gli effetti, senza che sia necessaria una nuova pubblicazione del Regolamento medesimo. Docenti e personale ATA sono tenuti a leggere, a conoscere e a seguire scrupolosamente le disposizioni previste nelle eventuali modifiche e integrazioni della procedura prevista per il caso di *Data breach*.

Art. 10 – Entrata in vigore e applicazione

Il presente Regolamento entra in vigore il giorno 1 luglio 2023.

In ragione delle specifiche peculiarità del mondo della scuola, le disposizioni del presente Regolamento divengono applicabili dal giorno 1 settembre 2023.

Verona, 23/06/2023

Il Dirigente scolastico
(Dott. Luigi Franco)
documento informatico firmato digitalmente ai sensi del D.Lgs. 82/2005 s.m.i. e norme collegate, il quale sostituisce il documento cartaceo e la firma autografa

POLICY

DATA BREACH

COD. C.07
VERS. 01 DEL 05.2022

CONTIENE:

1. **POLICY**

INDICE DELLE VERSIONI SUCCESSIVE ALLA PRIMA:

COD. VERSIONE	DATA MODIFICA	MODIFICHE

PREMESSA

Un data breach consiste in una violazione della sicurezza che comporta – accidentalmente o illegalmente – la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali, trasmessi, archiviati o

altrimenti elaborati. Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità dei dati personali.

- **Perdita di riservatezza**: quando un soggetto terzo accede o riceve dati a lui non destinati (esempi: accesso di hacker al server della scuola; invio di una mail ai genitori contenente dati sensibili di alcuni ragazzi).
- **Perdita di integrità**: quando un evento pregiudica l'integrità dei database (esempi: allagamento degli archivi, incendio in sala server).
- **Perdita di disponibilità**: quando a causa di un particolare evento è impedito al titolare di accedere ai dati (esempi: malware che rende inaccessibili le icone sul desktop).

È a tal riguardo importante evidenziare che il data breach può riguardare tanto i dati contenuti in supporto **cartaceo** che quelli contenuti in un supporto **digitale**. Tutti i data breach sono incidenti di sicurezza, ma non tutti gli incidenti di sicurezza sono necessariamente data breach.
La procedura di gestione del data breach non prevede che l'incaricato comunichi la violazione ad altri soggetti che non siano specificamente il Dirigente scolastico e il DPO (i.e. la Polizia postale). La procedura di gestione del data breach con notifica al Dirigente scolastico e al DPO deve sempre essere effettuata.

TIPOLOGIE RICORRENTI DI DATA BREACH

Alcuni casi tipici di violazione dei dati sono elencati di seguito:

- Furto delle credenziali di autenticazione ed utilizzo delle stesse
- Smarrimento di una chiavetta USB o di un cellulare o laptop con conseguente perdita di documenti contenenti dati personali
- Cancellazione accidentale
- Pubblicazione su internet di graduatorie contenenti dati sensibili
- Invio di dati sensibili a genitori
- Furto di documenti cartacei contenenti dati sensibili
- Accesso a informazioni riservate da parte di utenti non autorizzati

COME GESTIRE UN DATA BREACH. I PRIMI 10 MINUTI.

NOTA BENE: In caso di violazione dei dati, il Titolare ha un massimo di 72 ore per segnalare il problema al Garante.

In caso di incidente di sicurezza (verificato o sospetto), il dipendente/collaboratore della scuola dovrà procedere come segue:

1. Arresta la perdita di dati aggiuntiva: se si tratta di un data breach che coinvolge i sistemi elettronici, porta offline le macchine interessate, ma non spegnerle. Spegni il Wi-Fi o scollega il cavo ethernet dal laptop.
2. Chiamare immediatamente il DPO e il Dirigente scolastico.
3. Registrare il momento della scoperta: inviare una mail a rpd@euservice.it con le seguenti informazioni: chi ha scoperto la violazione, chi l'ha segnalata, a chi è stata segnalata, chi altro ne è a conoscenza e che tipo di violazione si è verificata.

È importante sottolineare che segnalare l'incidente al Dirigente scolastico e al DPO non deve costituire motivo di discriminazione dell'operato del personale ma è anzi il presupposto per il miglioramento della gestione dei dati dell'organizzazione. Più incidenti verranno registrati all'interno del registro delle violazioni, più potranno essere fatte delle formazioni puntuali e contestualizzate da parte del DPO e quindi più l'organizzazione migliorerà la gestione della privacy.
La legge chiede al Titolare di notificare la violazione all'Autorità Garante entro 72 ore dall'accaduto; tuttavia, qualora

l'incaricato al trattamento si rendesse conto di aver causato un data breach successivamente alle 72 ore ne dovrà dare comunicazione al Dirigente scolastico e al DPO non appena possibile. Infatti, è sempre meglio notificare la violazione, se dovuto, che non farlo perché una violazione scoperta *ex post* dall'Autorità potrà aggravare l'ammontare di eventuali sanzioni.

COME GESTIRE UN DATA BREACH. I SUCCESSIVI 10 MINUTI

Il soggetto (o i soggetti) che hanno scoperto la violazione dei dati devono scrivere un report al DPO contenente le seguenti informazioni:

- il database (anche cartacei) interessati, nonché la causa e l'entità;
- le categorie e il numero approssimativo delle persone interessate
- le categorie e il volume approssimativo dei dati personali interessati
- una descrizione delle possibili conseguenze della violazione dei dati personali
- possibilmente indicare se la violazione è partita dall'interno o dall'esterno della scuola

UNA E-MAIL CON LE SUDDETTE INFORMAZIONI DEVE ESSERE INVIATA IMMEDIATAMENTE AL DPO ALL'INDIRIZZO: rpd@euservice.it

NOTIFICA DI VIOLAZIONE

Il DPO valuterà, dopo aver effettuato l'analisi dei rischi, se si dovrà notificare l'Autorità Garante poiché le violazioni che **non presentano rischi per gli interessati** non dovranno essere notificate all'Autorità. In caso di comunicazione all'Autorità Garante bisognerà compilare apposito modulo presente sul sito dell'Autorità. Il modulo sarà compilato dal Dirigente scolastico, su consiglio del DPO, e trasmesso all'Autorità Garante da parte del Titolare del Trattamento entro un massimo di 72 ore. Se la notifica viene inviata dopo 72 ore, è necessario descrivere il motivo del ritardo. **Attenzione, le 72 ore non conoscono motivi di sospensione, continuando a decorrere anche in giorni quali Natale, Pasqua ed altre festività**. Per questo è necessario comunicare eventuali data breach al DPO anche se a ridosso di giorni solitamente non lavorativi. La notifica di data breach si effettua tramite apposito portale sul sito del Garante Privacy e raggiungibile al seguente indirizzo: https://servizi.gpdp.it/databreach/s/

La notifica dovrebbe contenere:

1. Una descrizione della natura della violazione dei dati personali, tra cui, se possibile:
   - Le categorie e il numero approssimativo delle persone interessate
   - Le categorie e il volume approssimativo dei dati personali interessati
2. Il nome e i dettagli di contatto del DPO o di una persona di contatto competente a fornire informazioni
3. Una descrizione delle possibili conseguenze della violazione dei dati personali
4. Una descrizione delle misure adottate o proposte per porre rimedio alla violazione dei dati personali, comprese, se del caso, le misure adottate per mitigare eventuali effetti negativi
5. Una descrizione dei motivi del ritardo se la notifica è stata effettuata dopo il limite di 72 ore.

Se è probabile che la violazione comporti un rischio elevato per la privacy o la sicurezza di un interessato, tali soggetti saranno informati entro 72 ore dalla scoperta della violazione. Per notificare un individuo colpito da una violazione dei dati personali, la natura della violazione dei dati sarà descritta in un linguaggio chiaro e semplice. Se il data breach è un incidente di tipo informatico bisognerà avvisare anche la Polizia Postale. Sarà necessario, inoltre, un dialogo particolarmente approfondito tra il DPO e l'Amministratore di sistema. Se l'incidente informatico rappresenta un rischio elevato per gli interessati e per la rete in generale sarà necessario contattare anche il CSirt (Computer security incident response team) per ricevere istruzioni in merito alla sua gestione.

Tutte le violazioni dei dati personali, indipendentemente dal ricorrere dell'obbligo o meno di segnalarle, saranno registrate dal DPO in un apposito registro (Registro degli incidenti di violazione dei dati), registrando:

- Chi ha notificato la violazione dei dati e data
- Descrizione della violazione dei dati
- Individuo colpito
- Effetti
- Azioni correttive intraprese e data di scadenza
- Se la violazione è stata notificata o meno al Garante

È bene ricordare che in caso di ispezione l'Autorità Garante potrà chiedere il registro delle violazioni che quindi deve essere compilato adeguatamente. Un registro delle violazioni vuoto o mal compilato potrebbe far generare dei sospetti all'Autorità che alla privacy non venga dato il giusto peso. A tal fine si allega un modello di registro di data breach da utilizzare per annotare le precedenti informazioni.

MODELLO REGISTRO DATA BREACH

DESCRIZIONE EVENTO	DATA E ORA EVENTO	FONTE NOTIZIA	TITOLARE TRATTAMENTO	DATA E ORA NOTIFICA	DOVE RINVENIRE PROVA NOTIFICA	PERCHÉ NON È STATO NOTIFICATO IL DATA BREACH	DATA E ORA DI COMUNICAZIONE AGLI INTERESSATI	CATEGORIA DI DATI OGGETTO DI VIOLAZIONE	CATEGORIA DI INTERESSATI COINVOLTI

Il registro dei data breach, una volta compilato dovrà essere munito di data certa, ad esempio, inviando dalla vostra pec alla vostra pec il documento stesso.

LICEO SCIENTIFICO STATALE "FRACASTORO"

Protocollo numero: ***5632 / 2023***
Data registrazione: ***23/06/2023***

Tipo Protocollo: ***USCITA***
Documento protocollato: ***Regolamento finalizzato alla mitigazione dei rischi derivanti dall'uso della piattaforma Google.pdf***
AOO: ***vrps03000r***
IPA: ***istsc_vrps03000r***

Oggetto: ***REGOLAMENTO FINALIZZATO ALLA MITIGAZIONE DEI RISCHI DERIVANTI DALL'USO DELLA PIATTAFORMA GOOGLE***

Destinatario:
AGLI ATTI ALL'ALBO
AMMINISTRAZIONE TRASPARENTE

Ufficio/Assegnatario:
FRANCO LUIGI (Ufficio Dirigenza)

Protocollato in:

Titolo: ***1 - AMMINISTRAZIONE***
Classe: ***4 - Archivio, accesso, privacy, trasparenza e relazioni con il pubblico***
Sottoclasse: ***- - -***

COPIA CONFORME ALL'ORIGINALE DIGITALE