MINISTERO DELL'ISTRUZIONE,
DELL'UNIVERSITA' E DELLA RICERCA

ISTITUTO DI ISTRUZIONE SUPERIORE "Guglielmo Marconi"

ANAGNI

- **ISTITUTO TECNICO COMMERCIALE E PER GEOMETRI** ***"G. Marconi"*** *sez. associata*
- **LICEO ARTISTICO** ***"G. Colacicchi"*** *sez. associata*
- **ITCG** ***"G. Marconi"*** *corso serale*
- **ITCG** ***"G. Marconi"*** *sez. carceraria Paliano*

Via Calzatora, 5 - 03012 Anagni (FR)
tel. 0775.727026 - fax 0775.739221
P.I. 80012420602 - FRIS01300B@istruzione.it

Procedura "DPIA"

"Data Protection Impact

Assessment" Regolamento UE

679/2016

			Prima Emissione	RPD Ing. Valeri Claudio	RTPD	Titolare del trattamento dei dati
Edizione 1	**Revisione**	**Data 28/02/2022**	**Descrizione Prima emissione**	**Redatto da DSGA A.Iafrate**	**Verificato da D.S. Prof.ssa Marilena Ciprani**	**Approvato da D.S. Prof.ssa Marilena Ciprani**

Approvato dal Consiglio di Istituto delibera n. 137 del 28/02/2020.

SOMMARIO

1.SCOPO

La presente procedura ha lo scopo di definire le modalità da seguire, ove richiesto, per una valutazione di impatto sulla protezione dei dati personali, definita “Data Protection Impact Assessment”, di seguito “DPIA”, e le relative responsabilità.

La valutazione d'impatto sulla protezione dei dati (DPIA, acronimo di Data Protection Impact Assessment) rappresenta l’output del processo di analisi del trattamento dei dati personali per l’Istituto “ IIS G. Marconi”. Questo documento è quindi un’analisi delle attività di trattamento attualmente gestite e delle relative valutazioni. Esso evidenzia i dettagli dell'attività di elaborazione stessa e fornisce una valutazione dei rischi associati al trattamento, suggerendo eventualmente le misure che possono essere adottate per mitigarli, anche grazie ad un’eventuale consultazione preliminare con il Responsabile per la Protezione dei Dati (RDP) competente.

Il titolare del trattamento elabora la DPIA ai sensi dell'articolo 35 del GDPR, laddove il trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche (l’interessato).

Questo documento, nelle sue varie parti:

- ***valuta i rischi per la privacy personale nei processi per l’Istituto “*IIS G. Marconi*”;***
- ***identifica le misure, le salvaguardie e i meccanismi esistenti o pianificati per garantire la protezione dei dati personali;***

identifica, ove ve ne sia necessità, il corretto bilanciamento tra i diritti alla privacy dell’individuo e quelli di raccolta ed elaborazione dei dati per finalità legittime dell’istituto “IIS G. Marconi”

1. CAMPO DI APPLICAZIONE

La procedura è applicabile a tutte le attività svolte dal Dirigente Scolastico Prof.ssa Marilena Ciprani (di seguito il titolare del trattamento), con particolare riferimento alla gestione di tutti gli archivi/documenti cartacei e di tutti i sistemi informatici attraverso cui vengono trattati dati personali degli interessati (clienti, fornitori, altri soggetti terzi, ecc.), anche con il supporto di fornitori esterni.

2. DEFINIZIONI E ABBREVIAZIONI

Definizioni

Per l'elenco completo, si rimanda all'Art. 4 del REGOLAMENTO (UE) 2016/679

1) ***«dato personale»:*** *qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno*

o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) ***«trattamento»:*** *qualsiasi operazione o insieme di operazioni ,compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;*

3) ***«limitazione di trattamento»:*** *il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;*

4) ***«profilazione»:*** *qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;*

5) ***«pseudonimizzazione»:*** *il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;*

6) ***«archivio»:*** *qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;*

7) ***«titolare del trattamento » :****la persona fisico giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamentodidatipersonali;quandolefinalitàeimezziditaletrattamentosonodeterminati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;*

8) ***«responsabile del trattamento»:*** *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;*

9) ***«destinatario»:*** *la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, leautoritàpubblichechepossonoriceverecomunicazionedidatipersonalinell'ambitodiuna specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;*

10) ***«terzo»:*** *la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone*

autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) ***«consenso dell'interessato»:*** *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;*

12) ***«violazione dei dati personali»:*** *la violazione di sicurezza che comporta 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;*

13) ***«dati genetici»:*** *i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;*

14) ***«dati biometrici»:*** *i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;*

15) ***«dati relativi alla salute»:*** *i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;*

16) «stabilimento principale»:

a) *per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbiafacoltàdiordinarel'esecuzioneditalidecisioni,nelqualcasolostabilimentoche ha adottato siffatte decisioni è considerato essere lo stabilimento principale;*

b) *con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;*

17) ***«rappresentante»:*** *la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;*

18) ***«impresa»:*** *la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;*

19) ***«gruppo imprenditoriale»:*** *un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;*

20) ***«norme vincolanti d'impresa»:*** *le politiche in materia di protezione dei dati personali applicatedauntitolaredeltrattamentooresponsabiledeltrattamentostabilitonelterritorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;*

21) ***«Autorità di controllo/Autorità»:*** *l'autorità pubblica indipendente istituita da uno Stato membro; in Italia è il Garante per la protezione dei dati personali.*

Abbreviazioni

RPD Responsabile per la protezione dei dati personali

RTDP Responsabile della tutela dei dati personali e della riservatezza dei dati aziendali (ove presente)

3. RESPONSABILITÀ

RPD	● Attuazione della DPIA dal supporto alla valutazione dei rischi sino ai controlli e relative azioni di adeguamento, quando necessarie. ● Valutazione dei rischi ed attuazione delle azioni di correzioni individuate.
Responsabile di Area / Servizio	
RTDP	● Supervisione del processo

4. MODALITÀ ESECUTIVE

Generalità

L'art. 35 del Regolamento, stabilisce che: Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, **una valutazione**

dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

Inoltre la norma prevede che: La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:
a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;o
c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

La Valutazione d'impatto o DPIA (Data Protection Impact Assessment) è una procedura finalizzata a descrivere un trattamento, valutare necessità e proporzionalità dello stesso, tenendo conto dei rischi per i diritti e le libertà delle persone fisiche derivanti da tale trattamento.

Attraverso la DPIA viene effettuata dal titolare la valutazione dei rischi e la definizione delle misure idonee ad affrontarli. La DPIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del Regolamento, ma anche a dimostrare l'adozione di misure idonee a garantire il rispetto di tali prescrizioni. La DPIA permette al Titolare di realizzare e dimostrare la conformità di uno specifico trattamento con le norme in materia di trattamento dei dati personali.

Necessità di effettuare la valutazione di impatto

Secondo le"Lineeguidaconcernentilavalutazionediimpattosullaprotezionedeidatinonché i criteri per stabilire se un trattamento possa presentare un rischio elevato ai sensi del regolamento 2016/679" del WP29, adottate il 4 ottobre 2017, per definire la necessità di effettuare la valutazione di impatto è opportuno prendere in esame i seguenti nove criteri:

1. *Valutazione o assegnazione di un punteggio, incluse la profilazione e la predizione, in particolare a partire da aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato (ad es. una banca che scremi i propri clienti tramite una banca dati di riferimento del credito, o una società di costruzione di profili comportamentali o di marketing in base all'utilizzo o alla navigazione sul suo sito web).*
2. *Decisioni automatiche con effetti giuridici o similmente significativi: elaborazione che mira a prendere decisioni su soggetti interessati e che produce effetti giuridici riguardanti*

la persona fisica o che allo stesso modo sia determinante per la persona fisica (ad es. il trattamento può comportare l'esclusione da determinati benefici).

3. *Controllo sistematico: trattamento utilizzato per osservare, monitorare o controllare soggetti interessati, inclusi i dati raccolti attraverso un controllo sistematico di una zona accessibile al pubblico.*
4. *Trattamento di dati particolari: si tratta delle categorie particolari di dati ai sensi dell'articolo 9 del GDPR (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonchédatigenetici,datibiometriciintesiaidentificareinmodounivocounapersona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona) oltre ai dati personali relativi a condanne penali o reati di cui all'art.10.*
5. *Trattamenti di dati elaborati su larga scala: il GDPR non definisce cosa costituisca larga scala, anche se il considerando 91 fornisce alcune indicazioni. In ogni caso, il WP29 raccomanda che i seguenti fattori, in particolare, siano considerati per determinare se il trattamento è effettuato su larga scala:*
    a. *il numero di persone interessate, come numero specifico o come percentuale della popolazione di riferimento;*
    b. *il volume dei dati e / o la gamma di diversi elementi di dati in corso di elaborazione;*
    c. *la durata, o la permanenza, dell'attività di elaborazione dati;*
    d. *l'estensione geografica delle attività di elaborazione.*
6. *Combinazione o raffronto di insiemi di dati, ad esempio provenienti da due o più trattamentieffettuatiperscopidiversie/odaaltrititolariinmodotaledasuperarele ragionevoli aspettative dell'interessato.*
7. *Trattamenti di dati relativi a interessati vulnerabili: il trattamento di questo tipo di dati può richiedere una DPIA a causa del maggiore squilibrio di potere tra interessato e titolare del trattamento, nel senso che il singolo può non essere in grado di acconsentire, o di opporsi, con facilità al trattamento dei propri dati, né può talora con facilità esercitare i propri diritti. La categoria degli interessati vulnerabili comprende anche i minori, i dipendenti, quei segmenti di popolazione particolarmente vulnerabile e meritevole di specifica tutela (soggetti con patologie psichiatriche, richiedenti asilo, anziani, pazienti) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento.*
8. *Utilizzi innovativi o applicazione di soluzioni tecnologiche o organizzative, come la combinazionefral'usodiimprontedigitalieilriconoscimentodelvoltoperunmigliore controllo di accesso fisico, ecc.*
9. *Trattamenti che impediscono agli interessati di esercitare un diritto o utilizzare un servizio o un contratto" (ad es. lo screening dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno a un finanziamento).*

Il WP29 ritiene che più sono i criteri inclusi nel trattamento, più è probabile che esso presenti un rischio elevato per i diritti e le libertà delle persone, e quindi richieda una DPIA. Come regola generale, un'operazione di elaborazione che includa meno di due criteri può non richiedere una DPIA per il minore livello di rischio, mentre operazioni di trattamento che soddisfino almeno due di questi criteri richiederanno una DPIA.

Metodologia

Il criterio utilizzato per l'analisi dei rischi, derivato con alcuni adattamenti dalla Norma DS/ISO/IEC 29134:2017 (Annex A) e dal documento "Privacy Impact Assessment" della Commission nationale de l'informatique et des libertés, 2015, si basa sulla correlazione fra la gravità (**G**) di un rischio (in relazione all'ampiezza degli impatti potenziali sugli interessati, tenendo conto delle misure esistenti) e la probabilità (**P**) di accadimento dell'evento che provoca il danno (in relazione alle vulnerabilità dei supporti interessati e alla capacità delle fonti di rischio di sfruttarle, tenendo conto delle misure esistenti).

A tal riguardo, si è definito l'indice di rischio **R** come funzione dell'Indice di probabilità per l'Indice di gravità del danno:

$$R = f(P, G)$$

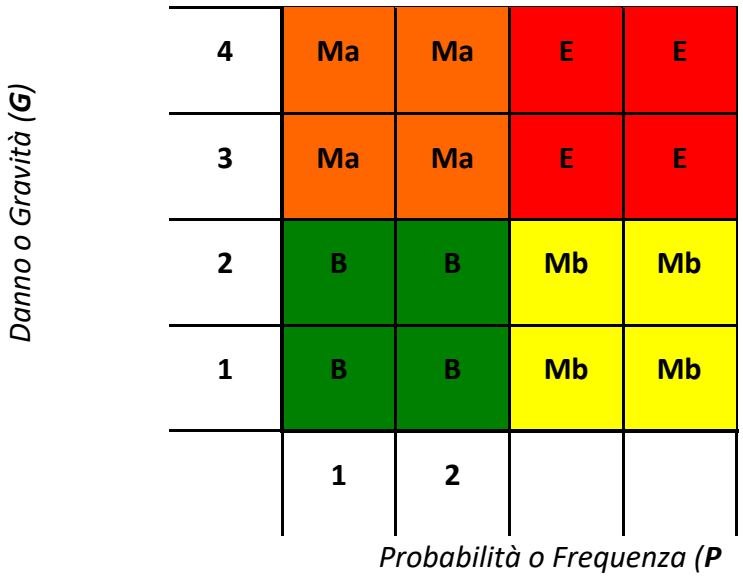
e, conseguentemente, la priorità da assegnare alle misure da adottare per ridurre il rischio ad un livello ritenuto accettabile.
Iriferimentiutilizzatiperunaoggettivarelazionefralivellievaloridigravitàeprobabilitàsono riportati di seguito.
*Gravità delle conseguenze per i diritti degli interessati (**G**) che il verificarsi dell'evento può produrre:*

- ***Livello 1 - Trascurabile: gli interessati non subiranno alcun impatto o potrebbero incontrare qualche inconveniente che supereranno senza difficoltà.***
- ***Livello2 - Limitato: gli interessati potrebbero sperimentare notevoli inconvenienti, che possono superare nonostante alcune difficoltà.***
- ***Livello 3 - Significativo: gli interessati potrebbe avere conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative.***
- ***Livello 4 - Massimo: gli interessati potrebbero avere conseguenze significative, anche irrimediabili, che potrebbero non essere superate.***

*Probabilità o Frequenza (**P**) con cui potrebbe verificarsi un evento:*

- ***Livello 1 - Trascurabile: non sembra possibile che le minacce possano concretizzarsi.***
- ***Livello 2 - Limitato: sembra difficile che le minacce possano concretizzarsi.***
- ***Livello 3 - Significativo: sembra possibile che le minacce possano concretizzarsi.***
- ***Livello 4 - Massimo: sembra molto facile che le minacce possano concretizzarsi.***

I Livelli di Rischio associabili alle diverse possibilità che possono verificarsi incrociando i livelli definiti di Probabilità e Gravità, si possono raggruppare in 4 Classi di Priorità secondo lo schema seguente:



- Priorità1-Livello di Rischio Elevato: questi rischi devono essere assolutamente evitati o ridotti applicando misure di sicurezza che ne riducano la gravità e la probabilità. Idealmente, dovrebbe anche essere garantito che vengano trattati contemporaneamente con misure di prevenzione (azioni prima del disastro), protezione (azioni durante il disastro) e recupero (azioni dopo il disastro).
- Priorità 2 - Livello di Rischio Medio alto: questi rischi devono essere evitati o ridotti applicando misure di sicurezza che ne riducano la gravità o la probabilità, favorendole misure. Possono essere presi, ma solo se si dimostra che non è possibile ridurre la loro gravità e se la loro probabilità è trascurabile.
- Priorità 3 - Livello di Rischio Medio basso: questi rischi devono essere ridotti applicando misure di sicurezza che riducano la loro probabilità, favorendo le misure di recupero. Possono essere presi, ma solo se si dimostra che non è possibile ridurre la loro probabilità e se la loro gravità è trascurabile.
- Priorità 4 - Livello di Rischio Basso: è possibile prendere questi rischi, soprattutto perché il trattamento di altri rischi porta anche al loro trattamento.

Attuazione della DPIA

Nel Registro delle attività di trattamento dei dati è inclusa, e deve essere aggiornata a cadenza al minimo annuale, una sezione nella quale sono individuati i trattamenti effettuati dal titolare

che richiedono un'analisi d'impatto.
In applicazione di tale determinazione sottoscritta dal Titolare, il RPD si attiva con le aree e/o servizi interessati per pianificare la specifica DPIA individuata come necessaria. Il responsabile di Area o di Servizio, con il supporto del RPD, elabora la valutazione dei rischi e definisce in accordo con il RPD le misure di controllo, compilando il documento "DPIA e piano di trattamento dei rischi" in Allegato1.

Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.
Quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento, il responsabile di Area o di Servizio, sentito il RPD, riesamina la valutazione dei rischi e le misure di controllo e aggiorna l'Allegato 1.

5. RIFERIMENTI

- REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del27aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)
- Decreto Legislativo 30 giugno 2003 n. 196, recante il Codice in materia di protezione deidatipersonalieprovvedimentiadottatidall'AutoritàGaranteperlaprotezionedei dati personali;
- Best practices di settore sviluppatesi alla luce del Codice e della giurisprudenza del Garante;
- Linee guida sulla notifica delle violazioni di dati personali ai sensi del Regolamento 679/2016 (WP250), adottate dal Gruppo di lavoro Articolo 29 ("WP29"), in via definitiva, il 6 febbraio2018;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento" possa presentare un rischio elevato" ai sensi del Regolamento 2016/679 (WP248), adottate dal WP29, in via definitiva, il 4 ottobre 2017;
- Linee guida sui responsabili della protezione dei dati (WP243), adottate dal WP29, in via definitiva, il 5 aprile2017;
- Dichiarazione relativa al ruolo di un approccio basato sul rischio nel quadro normativo in materia di protezione dati (WP218), adottata dal WP29 il 30 maggio2014;
- Raccomandazioni per una metodologia della valutazione della gravità delle violazioni di dati personali, adottate dalla European Union Agency for Network and Information Security (ENISA) il 20 dicembre2013;
- ISO 27001 "Information technology – Information security management systems - Requirements";

6. ARCHIVIAZIONE

I documenti allegati alla presente procedura sono archiviati da RPD.

7. MISURE DI SICUREZZA

Il Titolare del trattamento dei dati personali è tenuto ex art 24 GDPR, anche mediante l'adozione delle misure idonee e preventive di cui all'art. 31 D. Legisl. 196/03, ad adottare tutti gli accorgimenti in linea con le conoscenze acquisite in base al progresso tecnologico, al fine di custodire adeguatamente i dati altrui, prevenendone la perdita, la distruzione e l'accesso non autorizzato e comunque la protezione degli stessi a tutela dei diritti degli interessati. La mancata adozione delle misure idonee e preventive è atta a determinare una responsabilità di tipo civilistico verso gli interessati, con conseguente obbligo di risarcire gli eventuali danni causati da attacchi provenienti sia dall'interno che dall'esterno.

Dovranno pertanto essere adottati software antivirus e meccanismi di salvataggio dei dati, ma anche sistemi antincendio e di allarme nei locali ove sono contenuti i dati. Il problema dell'accesso non autorizzato comporta la necessità di apprestare difese preventive contro attacchi esterni provenienti dalle reti, ma anche contro accessi abusivi di personale interno non autorizzato per settore di competenza al trattamento, quali l'adozione di password differenziate in relazione agli utenti del sistema e nel conseguente tracciamento degli accessi.

Le misure idonee e preventive vanno tenute distinte dalle misure minime di sicurezza previste dall'art. 33 d.lgs. 196/03, la cui mancata adozione, ben più grave, comporta come conseguenza una sanzione penale (art. 169 d.lgs. 196/03). Le misure minime di sicurezza sono volte ad assicurare un livello minimo di protezione dei dati personali. Unico soggetto responsabile è il Titolare del trattamento dei dati Dirigente Scolastico Prof.ssa Marilena Ciprani.

Il trattamento di dati effettuato con strumenti elettronici è consentito solo se sono adottate le misure minime indicate dall'art. 34 d.lgs. 196/03:

1. autenticazione informatica;
2. adozione di procedure di gestione delle credenziali di autenticazione;
3. utilizzazione di un sistema di autorizzazione;
4. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o manutenzione degli strumenti elettronici;
5. protezione degli strumenti elettronici e dei dati rispetto a trattamenti e accessi non consentiti;
6. adozione di procedure per la custodia di copie di sicurezza e il ripristino della disponibilità dei dati e dei sistemi;
7. tenuta di un aggiornato documento programmatico sulla sicurezza (abrogato).

Il trattamento di dati personali effettuato senza l'ausilio di strumenti elettronici è consentito solo se sono adottate le seguenti misure minime indicate dall'art. 35 d.lgs. 196/03:

1. aggiornamento periodico dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati o alle unità organizzative;
2. previsione di procedure per un'idonea custodia di atti e documenti affidati agli incaricati per lo svolgimento dei relativi compiti;
3. previsione di procedure per la conservazione di determinati atti in archivi ad accesso selezionato e disciplina della modalità di accesso finalizzata all'identificazione degli incaricati.

9. ATTUALE SITUAZIONE RELATIVA ALLE MISURE DI SICUREZZA

Accesso fisico ai locali

L'accesso alla scuola avviene tramite una porta a vetri dotata di maniglia anti panico. Tale porta è chiusa a chiave fuori dell'orario di apertura della scuola.

Tutti i locali contenenti strumenti informatici sono posizionati al primo, secondo e terzo piano. Le porte di accesso a tali locali (porte taglia fuoco) vengono chiuse a chiave fuori dell'orario di lavoro.

Accesso fisico ai sistemi

Le postazioni informatiche della scuola sono solitamente poste sotto le scrivanie.

Il server della scuola è posizionato all'interno degli uffici amministrativi forniti di porta blindata di metallo, chiuse a chiave dopo l'orario di servizio. Il corridoio è video sorvegliato in orario extrascolastico. In caso di intrusione da parte di estranei, è funzionante un sistema di allarme sonoro collegato ai telefoni di personale dell'istituto, appositamente nominato

Accesso logico ai sistemi

Tutti i sistemi informatici della scuola sono dotati di un sistema di autenticazione (identificazione); tutti i sistemi o fanno parte di un dominio basato su un server Windows Microsoft (Active Directory) o hanno accesso con username e password locali.

Antivirus

Tutte le postazioni della scuola, sono dotate di un sistema antivirus che viene tenuto aggiornato periodicamente

Backup

1:

Il server della scuola è dotato di un sistema di backup dei dati che vengono salvati su un dispositivo dedicato posizionato in locale blindato, chiuso a chiave e dotato di allarme, in locale coincidente a quello dove è posizionato il server.

Tutte le altre postazioni della scuola non sono dotate di sistema di salvataggio.

Vengono fatti dei salvataggi estemporanei dei dati del server su dischi USB esterni criptati e conservati all' interno dell'edificio scolastico.

Disaster Recovery

I sistemi di backup consentono alla scuola il ripristino dei dati in caso di perdita o di disastro globale con attività svolte in autonomia o facendo intervenire la ditta esterna che gestisce il sistema di backup.

10. ALTRE MISURE DI SICUREZZA

Alimentazione elettrica

Il server è protetto da un sistema di continuità elettrica.

Gli altri apparati informatici non sono dotati di protezione contro le anomalie di alimentazione elettrica.

Accesso ad altre reti

La scuola accede alla rete internet tramite collegamenti ADSL, attraverso apparati UTM per firewalling, content-filtering e gestione autenticazione utenti wi-fi.

Anti incendio

In tutta la scuola esistono estintori e sono presenti sistemi di allarme e rilevazione automatica dei fumi. Non sono presenti sistemi di spegnimento automatico.

Applicazione correttivi ai sistemi

Su tutte le postazioni della scuola gli aggiornamenti di Windows vengono installati automaticamente. Sul server i correttivi per la sicurezza vengono installati manualmente alcune volte l'anno da personale qualificato.

Trattamenti cartacei

Presso gli uffici amministrativi della scuola esistono sia scaffali che armadi, alcuni dei quali dotati di serratura in cui vengono conservati i documenti. I documenti contenenti dati sensibili vengono conservati in armadi chiusi a chiave.

Telecamere e videosorveglianza

All'interno dell'Istituto sono state posizionate n.15 telecamere posizionate nei corridoi comuni come descritto nella tabella successiva, il cui scopo è quello di prevenire illeciti e/o danni alle cose e alle persone. Tali immagini vengono memorizzate (per un massimo di 5 giorni) su un apposito apparato posto nell'ufficio del Titolare. L' Istituto "Cardinale Oreste Giorgi" ha ben presente che il Garante Nazionale, dopo aver richiamato i principi generali del D.Lgs. 196/2003 e della Direttiva 95/46/CE, focalizzandoli sugli argomenti già affrontati nel proprio provvedimento generale sulla videosorveglianza dell'8 aprile 2010, ha chiarito che l'unica ipotesi di videosorveglianza attualmente ammessa è quella finalizzata alla tutela del patrimonio scolastico, purché le riprese siano effettuate durante le ore in cui non si svolge attività didattica.

Videocamere		Modalità
Quantità	Ubicazione	
7	I Piano	Visione e registrazione fuori orario didattico
8	PIANO TERRENO	Visione e registrazione fuori orario didattico

NALISI DEL RISCHIO (art 35 GDPR – Regola 19.3)

11. ***(TABELLA DA COMPLETARE)***

Evento			***Descrizione e impatto sulla sicurezza***	***Indice di probabilità***
C	E001	Sottrazione di credenziali di autenticazione	**Descrizione:** Le credenziali (es. Nome Utente/parola chiave) possono essere sottratte al legittimo possessore con vari metodi o scoperte anche grazie alla negligenza nella conservazione da parte del possessore stesso.	**1**
			Impatto: Altri soggetti possono accedere alle banche dati protette con tali credenziali sostituendosi in tutto e per tutto al soggetto possessore delle stesse. Il sistema di protezione non può in principio sapere dell'occorrenza di tale furto.	
	E002	Carenza di consapevolezza, disattenzione o incuria	**Descrizione:** A causa di impreparazione, anche tecnica, degli strumenti utilizzati e delle procedure messe a disposizione, gli incaricati del trattamento possono compiere operazioni errate.	**1**

omportamenti degli operatori			**Impatto:** Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati.	
	E003	Comportamenti sleali o fraudolenti	**Descrizione:** Con comportamento consapevole, derivante potenzialmente da vari fattori quali (risentimenti verso la scuola, il perseguimento di fini personali, etc.) gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati interessata l'evento.	**1**
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.	
	E004	Errore materiale	**Descrizione:** A causa di negligenza, scarsa conoscenza degli strumenti a disposizione o distrazione, gli incaricati del trattamento possono compiere operazioni errate o specificare dati errati.	**1**
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati.	
	E005	Comportamenti illegali a seguito di minacce	**Descrizione:** In conseguenza di pressioni di vario tipo (es. minacce, ricatti, pressioni psicologiche, ecc...) gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati interessata l'evento.	**1**
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.	
Eventi relativi agli	E101	Azione di virus informatici o di programmi suscettibili di recare danno	**Descrizione:** Sul sistema su cui si trova la banca dati interessata all'evento o il software utilizzato per accedervi, può introdursi un virus informatico o altro programma dannoso	**1**
			Impatto: Nei casi più gravi si può arrivare alla distruzione dell'intera banca dati. Nei casi meno gravi si può avere un malfunzionamento del sistema. In certi casi l'evento può comportare la sottrazione, in modo illecito, didati.	
strum	E102	Spamming o tecniche di sabotaggio	**Descrizione:** Il sistema di posta utilizzato dagli incaricati del trattamento potrebbe essere obiettivo di invii di posta non richiesta e fasulla generata anche con strumenti	**2**

e n ti			automatizzati. Tali messaggi possono contenere false notizie.	
			Impatto: Gli incaricati del trattamento possono erroneamente prendere in considerazione tali notizie ed operare interventi sulle banche dati non corretti.	
	E103	Malfunzionamento, indisponibilità degli strumenti	**Descrizione:** I sistemi HW/SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono avere malfunzionamenti da cui possono derivare impossibilità di azioni reali sui dati o creare inconsistenza nelle banche dati.	**1**
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati.	
	E104	Degrado degli strumenti	**Descrizione:** I sistemi HW/SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono essere soggetti a degrado naturale conseguente all'uso o al solo funzionamento. Da ciò possono derivare impossibilità di azioni reali sui dati o creare inconsistenza nelle banche dati.	**2**
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati.	
	E105	Accessi esterni non autorizzati	**Descrizione:** Soggetti in possesso di credenziali di accesso al sistema, o intenzionati a sferrare un attacco informatico ad uno dei sistemi HW/SW da cui è possibile intervenite su una banca dati obiettivo, possono accedere al sistema individuato da una postazione non utilizzata in condizioni normali di operatività per accedere a tale sistema.	**1**
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l evento può comportare la sottrazione, in modo illecito, di dati.	
	E106	Intercettazione di informazioni in rete	**Descrizione:** Soggetti malintenzionati possono catturare, mediante vari sistemi fisici, parte delle informazioni che transitano sulla rete informatica della scuola o sulla rete di collegamento con altri Enti. Ciò può avvenire in un qualunque punto tra il sistema utilizzato e il sistema HW/SW degli incaricati.	**1**

			Impatto: Nei casi più gravi, mediante varie tecniche, si può giungere alla distruzione o manipolazione dei dati. In generale si può avere una sottrazione di dati da parte dei malintenzionati.	
Eventi relativi al contesto	E201	Accessi non autorizzati a locali da cui è possibile accedere ai dati	**Descrizione:** Un soggetto autorizzato o non allo scopo, può comunque accedere fisicamente ai locali presso i quali è accessibile e manipolabile la banca dati interessata all'evento.	**1**
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.	
	E202	Sottrazione di strumenti contenenti dati	**Descrizione:** I sistemi HW/SW e/o i supporti di memorizzazione, nei quali sono memorizzati i dati relativi alla banca dati interessata all'evento, possono venire sottratti illecitamente da parte di altri soggetti non aventi diritto di accedere a tale banca dati.	**2**
			Impatto: L'evento comporta la sottrazione, in modo illecito, di dati.	
	E203	Eventi distruttivi, naturali o artificiali (movimenti tellurici, scariche atmosferiche, incendi, allagamenti, condizioni ambientali, ecc...), nonché dolosi, accidentali	**Descrizione:** I sistemi HW/SW e/o i supporti di memorizzazione, nei quali sono memorizzati i dati relativi alla banca dati interessata all'evento, possono essere interessati da eventi distruttivi di origine sia fortuita che dolosa. accidentali o volontari	**1**
			Impatto: Dall'evento può derivare la distruzione totale o parziale della banca dati o la sua indisponibilità fino al ripristino dei sistemi interessati all'evento.	
	E204	Guasto ai sistemi complementari	**Descrizione:** I sistemi ausiliari necessari al corretto funzionamento degli apparati HW/SW con i quali viene trattata o che contiene la banca dati interessata all'evento possono avere malfunzionamenti in conseguenza di varie cause.	**1**
			Impatto: Nei casi più gravi si può arrivare alla distruzione totale o parziale della banca dati. Nei casi meno gravi si ottiene la indisponibilità di tutta o parte della banca dati.	
	E205	Errori umani nella gestione	**Descrizione:** A seguito di errori umani è possibile causare malfunzionamenti ad apparati e sistemi, accessi non consentiti e altri danni alle strutture e ai dati.	**1**

		dell a sicurezza fisica	**Impatto:** Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.	

(TABELLA DA NON MODIFICARE)

Sistemi	***Evento***	***Probabilità*** ***(Bassa, Media, Alta)*** ***(da 0 a 3)***	***Gravità*** ***(Minima, Media, Massima)*** ***(da 0 a 3)***	***Rischio*** ***Probabilità x Gravità*** ***(valori 0,1,2,3,4,6,9)***
Tutti	E001	1	3	3
	E002	2	2	4
	E003	1	3	3
	E004	1	2	2
	E005	1	3	3
	E101	1	3	3
	E102	3	2	6
	E103	2	2	4
	E104	1	1	1
	E105	1	3	3
	E106	2	3	6

Sistemi	***Evento***	***Probabilità*** ***(Bassa, Media, Alta)*** ***(da 0 a 3)***	***Gravità*** ***(Minima, Media, Massima)*** ***(da 0 a 3)***	***Rischio*** ***Probabilità x Gravità*** ***(valori 0,1,2,3,4,6,9)***
	E201	1	3	3
	E202	2	3	6
	E203	1	3	3
	E204	2	2	4
	E205	1	3	3

12. MISURE DA ADOTTARE (art 35 GDPR – Regola 19.4)

Al fine di garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia ed accessibilità, devono essere adottate le seguenti misure:

- aggiornamento periodico (minimo una volta l'anno) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici con relativa segnalazione al titolare o al responsabile del trattamento

- mantenimento delle misure di prevenzione per eliminare gli eventuali incendi con adeguate modalità di gestione degli stessi (impianto elettrico a norma, idranti, estintori, disponibilità degli spazi per l'ingresso dei mezzi dei Vigili del Fuoco, etc.);

- regolamentazione nell'accesso ai locali e alle attrezzature che conservano dati, archivi e documentazione;

- i locali contenenti dati personali sensibili o giudiziari devono rimanere chiusi a chiave quando nessun incaricato è all'interno;

- valutazione di attuazione di misure di protezione attiva e passiva dei locali ove si trattano dati personali (sistemi allarme, porte di ferro, inferriate, protezione di accesso agli uffici di direzione, segreteria, archivio, sala insegnanti);

- controllo periodico del buon esito del salvataggio dei dati del server su unità rimovibili;

- istruzioni a tutti gli incaricati affinché non rimangano dati personali abbandonati sui singoli posti di lavoro;

- adozione di procedure per la custodia di copie di sicurezza e per il ripristino della disponibilità dei dati e dei sistemi in caso di distruzione o danneggiamento;

- periodica (almeno ogni tre mesi) verifica della funzionalità e dell'efficienza delle misure di protezione e delle strutture operative responsabili, anche mediante la compilazione di apposite schede di monitoraggio;

- adozione di procedure di gestione delle credenziali di autenticazione;

CRITERI, PROCEDURE PER GARANTIRE L'INTEGRITA' DEI DATI

Il Titolare del trattamento dei dati è il Dirigente Scolastico Marilena Ciprani, il quale stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche dei dati trattati. In particolare per ogni banca dati devono essere definite le seguenti specifiche:

- *il tipo di supporto da utilizzare per le copie di back-up;*
- *il numero di copie di back-up effettuate ogni volta;*
- *se i supporti utilizzati per le copie di back-up sono riutilizzati e in questo caso con quale periodicità;*
- *se per effettuare le copie di back-up si utilizzano procedure automatizzate e programmate;*
- *trasposizione dei dati informatici su unità rimovibili;*

- *la durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati;*
- *gli Incaricati del trattamento ai quali è stato assegnato il compito di effettuare le copie di back-up.*

CUSTODIA E CONSERVAZIONE DELLE COPIE DI BACK-UP

Le copie di back-up devono essere adeguatamente conservate a cura del Titolare del trattamento dei dati nell'armadio chiuso a chiave sito in amministrazione, con eventuale altra copia controllata da conservare all' esterno dell'Istituto scolastico. Tali siti di custodia delle copie di back-up devono essere protetti da:

- *Agenti chimici*
- *Fonti di calore*
- *Campi magnetici*
- *Intrusioni ed atti vandalici*
- *Incendio*
- *Allagamento*
- *Furto*

L'accesso ai supporti utilizzati per il back-up dei dati è limitato:

- *Al Titolare del trattamento*
- *Al Responsabile del trattamento della sicurezza dei dati*
- *Al tecnico informatico*

Quando il Titolare o il Responsabile del trattamento in sintonia con il tecnico informatico, decide che i supporti magnetici, utilizzati per le copie di back-up delle banche-dati, non sono più utilizzabili per gli scopi per i quali erano stati destinati, deve provvedere a farne cancellare il contenuto mediante completa formattazione.

PROTEZIONE DA VIRUS INFORMATICI

Al fine di garantire l'integrità dei dati contro i rischi di distruzione o perdita degli stessi a causa di virus informatici, il Titolare o il Responsabile del trattamento dei dati stabilisce, con il supporto del tecnico informatico, quali protezioni software adottare in relazione all'evoluzione tecnologica dei sistemi disponibili sul mercato.

Il Titolare del trattamento dei dati stabilisce inoltre la periodicità, di regola almeno semestrale, con la quale devono essere effettuati i controlli sugli aggiornamenti dei sistemi antivirus utilizzati, per ottenere un accettabile standard di sicurezza dei dati trattati.

E' opportuno che gli Incaricati che utilizzano i sistemi informatici annotino gli eventuali virus

rilevati, e, se possibile, la fonte da cui sono pervenuti, al fine di isolare o comunque trattare con precauzione i possibili portatori di infezioni informatiche.

Nel caso in cui su uno o più sistemi si dovesse verificare perdita di informazioni o danni a causa di infezioni o contagio da virus, l'Incaricato deve obbligatoriamente informare al più presto il Responsabile del trattamento che unitamente al tecnico informatico, deve provvedere a:

- Isolare il sistema
- Verificare se ci sono altri sistemi infettati con lo stesso virus informatico
- Identificare l'antivirus adatto e bonificare il sistema infetto
- Verificare il buon funzionamento dell'antivirus su tutti i sistemi
- Compilare un modulo di "Report dei contagi da virus informatici"
- Conservare in luogo sicuro i moduli compilati.

PROTEZIONE DELLE AREE E DEI LOCALI

La sicurezza di area è volta a prevenire accessi fisici non autorizzati, danni o interferenze con lo svolgimento dei servizi. Le contromisure si riferiscono alla protezione perimetrale dei siti, ai controlli fisici all'accesso, alla sicurezza degli archivi e delle attrezzature informatiche rispetto ai danneggiamenti accidentali o intenzionali, alla protezione fisica dei supporti.

Per tutto l'edificio scolastico dovrebbe essere valutata l'opportunità di proteggere lo stesso con:

- *misure attive e passive di protezione;*
- *un sistema di allarme;*
- *vetri antisfondamento, per le finestre del piano terra (per evitare danni, indebite intrusioni e per cautelare maggiormente la sicurezza e l'incolumità fisica dell epersone);*
- *adeguate serrature di sicurezza.*

CRITERI E PROCEDURE PER IL RIPRISTINO DELLA DISPONIBILITA' DEI DATI (art 35 GDPR – Regola 19.5)

Banca dati / data base / archivio dati	*Criteri e procedure per il salvataggio e il ripristino dei dati*	*Pianificazione delle prove di ripristino*

Dati presenti sul server	Salvataggio giornaliero su supporto esterno	Almeno 2 volte l'anno il Titolare o il Responsabile provvede a far eseguire da un tecnico informatico delle prove di ripristino dei dati
Dati presenti sulle postazioni di lavoro	Salvataggio ad ogni utilizzo su supporto esterno o mediante chiavette USB	Almeno 2 volte l'anno il Titolare o il Responsabile provvede a far trasferire sul server i dati eventualmente presenti sulle postazioni di lavoro

FORMAZIONE DEGLI INCARICATI (art 35 GDPR – Regola 19.6)

Al Titolare o al Responsabile del trattamento dei dati è affidato il compito di verificare ogni anno, entro il 30 settembre, i bisogni formativi di cui necessitano gli Incaricati, in particolare nel caso di introduzione di nuovi elaboratori, programmi o sistemi informatici. E' necessario tenere il personale continuamente informato e all'altezza dei compiti che deve espletare, per meglio conoscere i rischi che incombono sui dati, per avere una ottimale conoscenza delle misure di sicurezza e degli adeguati comportamenti da adottare, delle responsabilità circa i dati danneggiati, persi o distrutti.

Gli interventi formativi andranno offerti al momento dell'ingresso in servizio di personale nuovo, per immissione in ruolo o per trasferimento, in occasione dell'adozione di nuovi strumenti o dell'installazione di altri software. E' opportuno documentare gli interventi formativi.

Una adeguata informazione/formazione va offerta, sempre a cura del Responsabile, anche ai collaboratori scolastici.

Parimenti una informazione/formazione va estesa e organizzata dal Responsabile del trattamento nei confronti del personale docente.

Gli interventi formativi riguarderanno le disposizioni applicative del D. L.vo 196/2003.

PIANIFICAZIONE DEGLI INTERVENTI FORMATIVI PREVISTI

Descrizione sintetica degli interventi formativi	*Classi di incarico o tipologie di incaricati interessati*	*Tempi previsti*
Nozioni di base di sicurezza informatica. Presentazione del GDPR e approfondimento dei concetti di informativa, consenso, figure coinvolte. Presentazione delle misure minime di sicurezza e loro implementazione in una realtà scolastica.	Personale amministrativo Docenti e ATA	Entro dicembre 2020

TRATTAMENTI AFFIDATI ALL'ESTERNO (art 35 GDPR – Regola 19.7)

Nel caso di attività affidate a terzi che comportano il trattamento di dati, è necessario che la società a cui viene affidato il trattamento rilasci specifiche dichiarazioni o documenti, oppure assuma alcuni impegni, anche su base contrattuale, con particolare riferimento, ad esempio, a:

1. trattamento di dati ai soli fini dell'espletamento dell'incarico ricevuto;
2. adempimento degli obblighi previsti dal codice per la protezione dei dati personali;
3. rispetto delle istruzioni specifiche eventualmente ricevute per il trattamento dei dati personali o integrazione delle procedure già in essere;
4. impegno a relazionare periodicamente sulle misure di sicurezza adottate – anche mediante eventuali questionari e liste di controllo – e ad informare immediatamente il titolare del trattamento in caso di situazioni anomale o di emergenze.

Descrizione sintetica dell'attività "esternalizzata"	***Trattamenti di dati interessati***	***Soggetto esterno***	***Descrizione dei criteri e degli impegni assunti per l'adozione delle misure***
Gestione anagrafiche e servizio di assistenza tecnica	Dati personali	AVASERVICE srl	Il soggetto esterno dovrà dichiarare di ottemperare agli obblighi previsti dal GDPR per la protezione dei dati personali; dovrà inoltre relazionare annualmente sulle misure di sicurezza adottate ed allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.
Gestione personale Certificati di malattia Dati presenze personale	Dati personali anche sensibili	MIUR- INPS	Il soggetto esterno dovrà dichiarare di ottemperare agli obblighi previsti dal GDPR per la protezione dei dati personali; dovrà inoltre relazionare annualmente sulle misure di sicurezza adottate ed allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.

CERTIFICAZIONI RILASCIATE DAGLI ESTERNI (art. 42 e ss. GDPR)

Al momento non sono presenti certificazioni di esterni.

CONCLUSIONI

Il "DPIA" potrà essere integrato e aggiornato in qualunque periodo dell'anno.

Il legale rappresentante – Titolare del trattamento dei dati - si impegna ad adottare, ogni possibile misura destinata a salvaguardare la sicurezza dei dati personali, contenuti nei documenti cartacei o registrati mediante strumenti elettronici. Tali misure riguarderanno gli aspetti organizzativi, logistici e procedurali miranti ad evitare con ogni mezzo qualsiasi incremento di rischi di distruzione o perdita, anche accidentale, dei dati oggetto di trattamento, di accesso non autorizzato o di trattamento non consentito.

Il presente documento viene portato nel Collegio Docenti per riferire sulla sua avvenuta redazione, per informazione ai componenti, per la adozione ed assunzione di delibera, anche al fine di consentire al Titolare di attuare gli adeguamenti fisici, logistici, tecnologici ed informatici urgenti e necessari per le finalità previste dalla legislazione vigente.

Anagni, 28/02/2020

Il Titolare del Trattamento dei Dati

Il Dirigente Scolastico
Prof. ssa Marilena Ciprani