

<b>ISTITUTO COMPRENSIVO M. L. KING</b>	<b>D.P.I.A.</b>		Pagina 1 di 11
	<i>Data Protection Impact Assessment</i>		
Istituto Comprensivo 'M.L.King' Pistoia Prot. 0005328 del 24/11/2021 08 (Entrata)			
<b>Sede direzionale / amministrativa</b>		<b>ISTITUTO COMPRENSIVO STATALE MARTIN LUTHER KING</b>	
Indirizzo	Via Ferdinando Santi n.1 - 51100 Pistoia (PT)		
Tel. /Fax.	0573544741		
E-mail/ Sito web	<a href="mailto:ptic809001@istruzione.it">ptic809001@istruzione.it</a>	<a href="http://www.istitutomartinlutherking.edu.it">www.istitutomartinlutherking.edu.it</a>	
C.F.	90026310475		

# D.P.I.A. - DATA PROTECTION IMPACT ASSESSMENT

**Relativa al trattamento dei dati necessari per la  
realizzazione di attività didattiche a distanza**

<b>Data</b>	<b>Motivo della revisione</b>	<b>Titolare del Trattamento (DS)</b>	<b>Responsabile della Protezione Dati (RPD)</b>
23/11/2021	Redazione della DPIA in conformità alla Nota del MIUR 388.17-03-2020	Dott.ssa Manila Cherubini	Ing. Alessandro Ottanelli

ISTITUTO COMPRENSIVO M. L. KING	D.P.I.A.	Pagina 2 di 11
	<i>Data Protection Impact Assessment</i>	

## INDICE

1. INTRODUZIONE.....	3
2. VALUTAZIONE PRELIMINARE.....	5
3. GESTIONE DEI RISCHI .....	6
4. CONCLUSIONI.....	11

<b>ISTITUTO COMPRENSIVO M. L. KING</b>	<b>D.P.I.A.</b>	Pagina 3 di 11
	<i>Data Protection Impact Assessment</i>	

## **1. INTRODUZIONE**

Questo documento è una valutazione dell'impatto sulla protezione dei dati (DPIA – Data Protection Impact Assessment) dell'Istituto in intestazione. La DPIA è un'analisi delle attività di trattamento previste e descrive i dettagli delle attività di trattamento sottoposte ad analisi ed una valutazione dei rischi associati alle stesse, comprese eventuali misure che devono essere adottate per mitigare tali rischi entro limiti accettabili.

Questa DPIA viene eseguita in accordo al requisito riportato nell'Art. 35 del Regolamento Europeo UE 2016/679, che prevede che, nel caso in cui un trattamento possa comportare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare del trattamento debba effettuare una valutazione di impatto del trattamento previsto, al fine di procedere o meno con l'effettuazione dello stesso. Nel caso di rischi "residui" elevati dopo l'adozione delle misure volte a mitigare gli stessi, il Titolare è tenuto a comunicare all'Autorità Garante della Privacy l'esito di tali valutazioni e, prima di procedere con l'effettuazione delle stesse, attendere il riscontro dell'Autorità Garante.

La redazione della presente DPIA si rende necessaria in quanto prevista dalla Nota del MIUR 388.17-03-2020, avente per oggetto "emergenza sanitaria da nuovo Coronavirus. Prime indicazioni operative per le attività didattiche a distanza."

Infatti, secondo quanto previsto dalle disposizioni normative vigenti in materia di contenimento e gestione dell'emergenza epidemiologica da COVID-19, i Dirigenti scolastici sono tenuti a attivare, per tutta la durata della sospensione delle attività didattiche nelle scuole, modalità di didattica a distanza avuto anche riguardo alle specifiche esigenze degli studenti con disabilità.

**La presente DPIA valuta i rischi relativi al trattamento di dati personali, in relazione all'utilizzo di piattaforme per la didattica a distanza.**

### DETTAGLI DEL PROGETTO DPIA

La tabella seguente mostra le informazioni di base del Progetto DPIA:

**TABELLA 1**

DESCRIZIONE E SCOPO DELLA DPIA	LA PRESENTE VALUTAZIONE DI IMPATTO E' EFFETTUATA DALL'ISTITUTO IN INTESTAZIONE ALLO SCOPO DI VALUTARE L'IMPATTO SUI DIRITTI E LIBERTA' DEGLI ALLIEVI DELLA SCUOLA E DEI DIPENDENTI, DOVUTI AI RISCHI RELATIVI AL TRATTAMENTO DEI DATI PERSONALI DEGLI STESSI NELL'ESECUZIONE DI MODALITÀ DI DIDATTICA A DISTANZA, UTILIZZANDO SPECIFICHE PIATTAFORME
PERSONE INTERESSATE E TIPOLOGIE DI DATI PERSONALI TRATTATI	LA VALUTAZIONE DI IMPATTO (DPIA) È EFFETTUATA PER LE SEGUENTI TIPOLOGIE DI "INTERESSATI" E DI RELATIVI DATI PERSONALI: <ul style="list-style-type: none"> <li>• ALLIEVI (DATI "COMUNI" (NOME E COGNOME, INDIRIZZI E-MAIL, ECC) E EVENTUALI RIPRESE MULTIMEDIALI (FOTO/VIDEO) IN OCCASIONE DI VIDEO-LEZIONI, EFFETTUATE SIA IN MODALITÀ SINCRONA, SIA ASINCRONA</li> <li>• DIPENDENTI (DATI "COMUNI" (NOME E COGNOME, INDIRIZZI E-MAIL, ECC) E EVENTUALI RIPRESE MULTIMEDIALI (FOTO/VIDEO) IN OCCASIONE DI VIDEO-LEZIONI, EFFETTUATE SIA IN MODALITÀ SINCRONA, SIA ASINCRONA)</li> </ul>
FINALITÀ DEL TRATTAMENTO	I DATI DEGLI ALLIEVI SONO TRATTATI AL FINE DI ATTIVARE LE PIATTAFORME PER L'EROGAZIONE DELLA DIDATTICA A DISTANZA.
MINIMIZZAZIONE ED AGGIORNAMENTO DEI DATI	I DATI RACCOLTI SONO ADEGUATI, RILEVANTI E LIMITATI A QUANTO NECESSARIO IN RELAZIONE ALLE FINALITÀ DEL TRATTAMENTO. I DATI SONO COSTANTEMENTE AGGIORNATI IN BASE ALLE EVENTUALI VARIAZIONI RISCOstrate
PERIODO DI CONSERVAZIONE DEI DATI	I DATI SARANNO CONSERVATI PER I TEMPI NECESSARI ALLO SVOLGIMENTO DELL'ATTIVITÀ DI DIDATTICA A DISTANZA E/O SECONDO QUANTO PREVISTO DALL'ALLEGATO I "PIANO DI CONSERVAZIONE E SCARTO PER GLI ARCHIVI DELLE ISTITUZIONI SCOLASTICHE" DEL D.P.R. 8 MARZO 1999, N.275.
MODALITÀ DI "ATTO DI INFORMAZIONE" ADOTTATA	ATTO DI INFORMAZIONE IN FORMATO CARTACEO (O ELETTRONICO) CONFORME AL REGOLAMENTO UE (CONTENENTE IN DETTAGLIO LE CARATTERISTICHE DEI TRATTAMENTI ED I DIRITTI DEGLI INTERESSATI) EMESSE DAL TITOLARE AL MOMENTO DELL'ISCRIZIONE. AI SENSI DELLA NOTA DEL MIUR 388.17-03-2020, L'ISTITUZIONE SCOLASTICA NON DEVE RICHIEDERE IL CONSENSO PER EFFETTUARE IL TRATTAMENTO DEI DATI PERSONALI (GIÀ RILASCIATO AL MOMENTO DELL'ISCRIZIONE) CONNESSI ALLO SVOLGIMENTO DEL LORO COMPITO ISTITUZIONALE, QUALE LA DIDATTICA, SIA PURE IN MODALITÀ "VIRTUALE" E NON NELL'AMBIENTE FISICO DELLA CLASSE.
DESTINATARI DEI DATI TRATTATI	I DATI VENGONO CARICATI SULLE PIATTAFORME PER L'EROGAZIONE DEI CONTENUTI DIDATTICI A DISTANZA. NON SONO PREVISTI DESTINATARI DI DATI DIVERSI DAI GESTORI DELLE PIATTAFORME STESSE.
COMUNICAZIONE DATI AL DI FUORI DELL'UE	NON È PREVISTO IL TRASFERIMENTO DI DATI ALL'ESTER

## 2. VALUTAZIONE PRELIMINARE

Il Titolare del trattamento, con il supporto del Responsabile per la protezione dati, ha effettuato una analisi preliminare sulla necessità o meno di condurre una **Valutazione di Impatto (DPIA – “Data Protection Impact Assessment”)** sulla protezione dei dati personali, adottando come guida la Tabella 2 seguente, tratta dai “criteri da considerare secondo il Gruppo di Lavoro Art. 29 (WP 29)”

### TABELLA 2

CRITERI DA CONSIDERARE SECONDO IL GRUPPO DI LAVORO ART. 29 (WP 29) QUANDO SI IDENTIFICA UN RISCHIO ELEVATO (CHE RICHIEDE L'IMPEGNO DI UNA PIA)

I TRATTAMENTI SONO RIFERITI AI SEGUENTI CRITERI?	SI	NO
1. Valutazione o punteggio, inclusa la profilazione e la previsione		X
2. Processo decisionale automatizzato con effetto significativo legale o simile		X
3. Monitoraggio sistematico (es. videosorveglianza su larga scala)		X
4. Dati sensibili, giudiziari, etc.		X
5. Dati trattati su larga scala	X	
6. Set di dati che sono stati abbinati o combinati		X
7. Dati riguardanti soggetti vulnerabili (minori)	X	
8. Uso innovativo o applicazione di soluzioni tecnologiche o organizzative (es: riconoscimento facciale, etc)		X
9. Quando l'elaborazione in sé "impedisce agli interessati di esercitare un diritto o di utilizzare un servizio o un contratto (es: selezione clienti banca per concessione finanziamento)		X

**Il Gruppo di Lavoro Art. 29 suggerisce di effettuare una DPIA se almeno 2 (due) dei criteri di cui sopra sono soddisfatti**

La valutazione preliminare conferma quindi che almeno due criteri della tabella precedente sono soddisfatti, pertanto il Titolare del trattamento, con il supporto del Responsabile per la protezione dei dati, ha ritenuto di effettuare una esaustiva **Valutazione di Impatto (DPIA) sulla protezione dei dati personali**, con l'impegno di rivederla periodicamente (in caso di variazione significativa dei dati trattati o del loro trattamento o almeno con cadenza annuale).

<b>ISTITUTO COMPRENSIVO M. L. KING</b>	<b>D.P.I.A.</b>	Pagina 6 di 11
	<i>Data Protection Impact Assessment</i>	

### **3. GESTIONE DEI RISCHI**

Nel valutare l'adeguato livello di sicurezza dei dati, si è tenuto conto dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.

#### ANALISI DEI RISCHI

Sono state individuate le seguenti risorse sulle quali condurre le analisi:

#### RISORSE:

HW  
SW  
RETI  
DATI (cartacei / multimediali / supporti magnetici)  
PERSONALE  
INFRASTRUTTURE

Per ciascuna delle risorse di cui sopra sono state individuate le minacce ed i fattori di rischio per la sicurezza dei dati, per i quali si è provveduto ad individuarne il relativo impatto utilizzando il metodo FMEA (Failure Mode Effect Analysis).

I risultati delle analisi sono riportati nella seguente Tabella 3.

**TABELLA 3**

SIGNIFICATO DEGLI INDICI E CRITERI DI VALUTAZIONE

<b>P = INDICE DI PROBABILITÀ</b>		
Altissima		9 - 10
Alta		7-8
Media		5-6
Bassa		3-4
Bassissima		1-2
<b>G = INDICE DI GRAVITÀ</b>		
Altissima		9 - 10
Alta		7-8
Media		5-6
Bassa		3-4
Bassissima		1-2
<b>IRR = P x G = INDICE DI RISCHIO RESIDUO</b>		
CRITERI DI VALUTAZIONE	<b>IRR ≤ 60 (BASSO)</b>	<b>NESSUNA AZIONE (MONITORAGGIO)</b>
	<b>IRR &gt; 61 (MEDIO/ALTO)</b>	<b>AZIONI DA STABILIRE ED EFFETTUARE</b>

NOTA: Nel caso di superamento di una determinata soglia dell'Indice di Rischio Residuo (IRR) considerata come "critica" sono previste ulteriori azioni per prevenzione / contenimento / riduzione dell'effetto indesiderato. Non vengono previste azioni nel caso di rischio considerato "basso": in tal caso viene comunque eseguito un "monitoraggio" continuo del livello dell'indice.





### VALUTAZIONE DEI RISCHI

RISORSE	MINACCE	RISCHI	PROVVEDIMENTI GIÀ IN ATTO	INDICE DI RISCHIO RESIDUO			AZIONI DA ATTUARE
				P	G	IRR	
<b>HW</b> <b>(fisso e mobile)</b>	Guasti, sabotaggi, Perdita accidentale Uso non autorizzato Malfunzionamento e/o carente manutenzione Guasto a sistemi complementari (impianto elettrico, etc.)	Perdita e/o divulgazione di dati a non autorizzati, con potenziale impatto sui diritti e le libertà degli interessati (es "stigmatizzazione", "emarginazione", "trattamento differenziato", etc.)	Utilizzo di apparecchiature a norma, nel rispetto di quanto stabilito nel manuale d'uso Accesso protetto mediante autenticazione personale Personale adeguatamente istruito circa le corrette procedure di accesso alle piattaforme e circa le corrette procedure di trattamento dei dati	3	4	12	<b>NESSUNA</b> <b>(MONITORAGGIO)</b>
<b>SW</b> <b>(su sistemi fissi e mobili)</b>	Azione di virus informatici o di codici malefici Spamming o tecniche di sabotaggio Uso improprio / errato del software Manomissione del SW Corruzione dei dati Falsificazione diritti di accesso Trattamento illecito dei dati Furto o copia del software	Perdita, danneggiamento e/o divulgazione di dati a non autorizzati con potenziale impatto sui diritti e le libertà degli interessati (es "stigmatizzazione", "emarginazione", "trattamento differenziato", etc.)	PC protetti da antivirus / firewall Back-up e ripristino dati Accesso protetto mediante autenticazione personale Personale adeguatamente istruito circa le corrette procedure di accesso alle piattaforme e circa le corrette procedure di trattamento dei dati	5	4	20	<b>NESSUNA</b> <b>(MONITORAGGIO)</b>
<b>RETE</b>	Azione di virus informatici o di codici malefici Spamming o tecniche di sabotaggio Uso improprio / errato della rete Trattamento illecito dei dati Furto o copia dei dati	Perdita, danneggiamento e/o divulgazione di dati a non autorizzati con potenziale impatto sui diritti e le libertà degli interessati (es "stigmatizzazione", "emarginazione", "trattamento differenziato", etc.)	PC protetti da antivirus / firewall Back-up e ripristino dati Accesso protetto mediante autenticazione personale Personale adeguatamente istruito circa le corrette procedure di accesso alle piattaforme e circa le corrette procedure di trattamento dei dati	5	4	20	<b>NESSUNA</b> <b>(MONITORAGGIO)</b>

RISORSE	MINACCE	RISCHI	PROVVEDIMENTI GIÀ IN ATTO	INDICE DI RISCHIO RESIDUO			AZIONI DA ATTUARE
				P	G	IRR	
<b>DATI MULTIMEDIALI (VIDEO/FOTO)</b>	Azione di virus informatici o di codici malefici Spamming o tecniche di sabotaggio Uso improprio / errato della rete Trattamento illecito dei dati Furto o copia dei dati Furto/copia dei dati Diffusione non autorizzata in rete	Perdita, danneggiamento e/o divulgazione di dati a non autorizzati con potenziale impatto sui diritti e le libertà degli interessati (es "stigmatizzazione", "emarginazione", "trattamento differenziato", etc.)	PC protetti da antivirus / firewall Back-up e ripristino dati Accesso protetto mediante autenticazione personale Personale adeguatamente istruito circa le corrette procedure di accesso alle piattaforme e circa le corrette procedure di trattamento dei dati	5	5	25	<b>NESSUNA (MONITORAGGIO)</b>
<b>PERSONALE</b>	Scarsa consapevolezza o conoscenza del problema della sicurezza Sottrazione e divulgazione credenziali di autenticazione Carenza di consapevolezza, disattenzione o incuria Comportamenti sleali o fraudolenti Errori materiali	Perdita, danneggiamento e/o divulgazione di dati non autorizzati con potenziale impatto sui diritti e le libertà degli interessati (es "stigmatizzazione", "emarginazione", "trattamento differenziato", etc.)	Accesso protetto mediante autenticazione personale Obbligo agli operatori di custodire e di non divulgare i dispositivi di accesso agli strumenti informatici Personale adeguatamente istruito circa le corrette procedure di accesso alle piattaforme e circa le corrette procedure di trattamento dei dati	3	4	12	<b>NESSUNA (MONITORAGGIO)</b>

<b>ISTITUTO COMPRENSIVO M. L. KING</b>	<b>D.P.I.A.</b>	Pagina 11 di 11
	<i>Data Protection Impact Assessment</i>	

### RISCHI RESIDUI

L'analisi dei rischi documentata nella Tabella 3 precedente mostra, per ciascuna risorsa considerata, un livello di rischio residuo ACCETTABILE per permettere la gestione dei trattamenti oggetto della presente DPIA.

Il Titolare del Trattamento, con il parere favorevole del Responsabile per la protezione dati, ritiene di:

- Non aver rilevato rischi residui elevati, tali da comportare una segnalazione al Garante della Privacy prima di effettuare i trattamenti oggetto della presente DPIA;

### **4. CONCLUSIONI**

Il Titolare del Trattamento, con il parere favorevole del Responsabile per la protezione dati, ritiene di:

- Procedere ai trattamenti oggetto della presente DPIA, monitorando costantemente i fattori di rischio e continuando ad adottare le misure tecniche ed organizzative atte alla riduzione dei rischi relativi ai trattamenti in oggetto;
- Programmare una revisione della presente DPIA in caso di variazione significativa dei dati trattati o del loro trattamento o almeno con cadenza biennale.

PISTOIA, 23/11/2021

Il Titolare del trattamento (DS)

Dott.ssa Manila Cherubini

Firma: \_\_\_\_\_

Il Responsabile protezione dati (RPD)

Ing. Ottanelli Alessandro

Firma:  \_\_\_\_\_