

**Ministero dell'Istruzione, dell'Università e della Ricerca**

Ambito Scolastico CE/7

**ISTITUTO COMPRENSIVO STATALE**

**"COLLECINI - GIOVANNI XXIII"**

**SAN LEUCIO - CASTEL MORRONE**

SCUOLA DELL'INFANZIA - SCUOLA PRIMARIA

SCUOLA SECONDARIA DI PRIMO GRADO AD INDIRIZZO MUSICALE

Via Giardini Reali n. 44 - 81100 Caserta

Tel. 0823/1444425 -

Codice Ministeriale CEIC80800N - Codice Fiscale 93036920614

Sito Web: [www.collecini.edu.it](http://www.collecini.edu.it)

E-Mail: [ceic80800n@istruzione.it](mailto:ceic80800n@istruzione.it) - Pec: [ceic80800n@pec.istruzione.it](mailto:ceic80800n@pec.istruzione.it)



**VALUTAZIONE D' IMPATTO ( DPIA-Data Protection Impact Assessment)**

**"per le attività di prevenzione e gestione dei fenomeni di Cyberbullismo"**

**INDICE**

1	Versioni e revisioni .....	2
2	Informazioni DPIA.....	2
3	Livello di riservatezza del documento.....	2
4	Parere Interessati .....	3
5	Contesto Panoramica del trattamento.....	3
6	Responsabilità connesse al trattamento.....	3
7	Standard applicabili al trattamento.....	3
8	Descrizione sistemica del trattamento.....	3
8.1	Dati, processi e risorse di supporto.....	3
9	Principi Fondamentali .....	4
9.1	Proporzionalità e necessità .....	4
10	Misure a tutela dei diritti degli interessati .....	5
11	Rischi Misure esistenti o pianificate.....	6
12	Accesso illegittimo ai dati.....	7
13	Modifiche indesiderate dei dati.....	8
14	Perdita di dati.....	8

## VALUTAZIONE D' IMPATTO ( DPIA-Data Protection Impact Assessment)

“per le attività di prevenzione e gestione dei fenomeni di Cyberbullismo”

### 1 Versioni e revisioni

REVISIONE	DATA Inizio	MODIFICHE APPORTATE	DATA VERIFICA	DATA VALIDAZIONE
001	05.06.2019	Prima stesura Inizio elaborazione del documento		

### 2 Informazioni DPIA

<b>Soggetto tenuto a condurre la DPIA</b>	Titolare del Trattamento I. C. Collecini –Giovanni XXIII Codice Ministeriale CEIC80800N
<b>Redattore</b>	Responsabile della Protezione dei dati avv. Monica Ragone
<b>Verificatore interno</b>	DSGA Dott.ssa Amalia Russo
<b>Validatore</b> ( in persona del legale rapp.te p.t. )	I.C. Collecini-Giovanni XXIII Nella persona del Dirigente Scolastico Prof. Antonio Varriale

### 3 Livello di riservatezza del documento

Livello	Ambito di diffusione consentito
Uso Pubblico	Il documento nella sua versione completa può essere pubblicato sul sito istituzionale. . E' necessario inviare il documento in forma completa all'autorità di controllo in caso di consultazione preventiva ovvero su richiesta dell'autorità stessa.

#### 4 Parere Interessati

<b>Richiesta parere degli interessati</b>	Non è stato chiesto il parere degli interessati.
<b>Motivazione della mancata richiesta del parere degli interessati</b>	Non si è ritenuto necessario richiedere un parere agli interessati, trattandosi di un trattamento necessario ai fini di legge.

#### 5 Contesto Panoramica del trattamento

Il trattamento consiste nella raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, e la comunicazione mediante trasmissione dei dati personali degli interessati, a fini di prevenzione ed eventuale gestione dei fenomeni di cyberbullismo connessi con le attività della scuola.

#### 6 Responsabilità connesse al trattamento

Il titolare del trattamento è l' I.C. Collecini – Giovanni XXIII. Si prevede la condivisione dei dati con l'autorità giudiziaria, su richiesta esplicita della stessa. I dati relativi ad episodi di cyberbullismo di cui la scuola viene a conoscenza potrebbero, qualora fosse necessario e ai fini delle indicazioni dell'Art. 5 della Legge 71/2017, essere condivisi con gli interessati o con i genitori degli stessi.

Responsabile del trattamento è il gestore del software e del server di conservazione connesso al servizio di segreteria digitale scolastico.

#### 7 Standard applicabili al trattamento

Non si rilevano standard applicabili al trattamento oggetto della presente Valutazione d' Impatto.

#### 8 Descrizione sistemica del trattamento

##### 8.1 Dati, processi e risorse di supporto

<b>Tipologia di dati</b>	Dati anagrafici di alunni , genitori e dipendenti della scuola . Eventuali dati personali degli esperti che prestano attività formativa in materia
<b>Ciclo di vita del Trattamento</b>	I dati di alunni, genitori e dipendenti provengono dagli archivi scolastici, e vengono conservati per la durata dell'evento o per i relativi adempimenti di legge. Le eventuali chat o post su social network dei quali l'amministrazione viene messa a conoscenza, relativi ad episodi di cyberbullismo, vengono acquisiti dalla scuola ai fini dell'adempimento agli obblighi relativi alla normativa vigente , e mantenuti nella esclusiva disponibilità del Dirigente Scolastico (D.S.) o di un suo eventuale delegato (ad es ., a discrezione del D.s., il referente scolastico per il cyberbullismo così come introdotto nell'Art. 4, comma 3 della Legge 71/2017). I dati degli esperti esterni incaricati delle attività formative in materia

	vengono trattati secondo le modalità descritte nel registro dei trattamenti, relative al trattamento di dati personali di esperti esterni alla scuola.
<b>Risorse di supporto ai dati</b>	I dati di alunni, genitori, dipendenti ed esperti esterni vengono trattati facendo uso delle risorse informatiche della scuola. L'hardware utilizzato consiste nelle risorse hardware scolastiche (PC del D.S., ed eventualmente del referente per il cyberbullismo o della segreteria per le attività di protocollo), il software utilizzato consiste nella suite di segreteria digitale scolastica. Le eventuali chat o post inerenti atti di cyberbullismo vengono acquisiti dalla scuola e conservati con accesso riservato al D.S. e al suo eventuale delegato (referente per il cyberbullismo).

## 9 Principi Fondamentali

### 9.1 Proporzionalità e necessità

<b>Gli scopi del trattamento sono specifici, espliciti e legittimi?</b>	Il trattamento viene effettuato ai fini del perseguimento di un obbligo legale dell'amministrazione, orientato specificamente alla prevenzione e/o gestione degli episodi di cyberbullismo.
<b>Quali sono le basi legali che rendono lecito il trattamento?</b>	Le basi legali sono da ricercarsi nella Legge 71/2017 (Disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo). Il trattamento si profila inoltre come attività di interesse pubblico rilevante, di istruzione e formazione in ambito scolastico, professionale, superiore o universitario, come previsto dall' art. 6 lett. e del Regolamento Europeo 679/2016 ed art. 9 lett. g del Regolamento Europeo 679/2016 Inoltre, le modalità di archiviazione sono definite da: il DPR 445/2000; Decreto Legislativo 22 gennaio 2004 n. 42, Codice dei beni culturali e del paesaggio Legge 6 luglio 2002, n. 137, art 10 (G.U. n. 45 del 24 febbraio 2004, s.o. n. 28).
<b>I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?</b>	Per la realizzazione delle attività di formazione e prevenzione non vengono utilizzati dati in eccesso rispetto a quelli già esistenti negli archivi scolastici. Qualora venissero individuati atti di cyberbullismo all'interno del campo di influenza dell'amministrazione scolastica, si prevede di acquisire le informazioni minime per

	l'esercizio degli obblighi legali, limitando al tempo stesso l'accesso alle stesse al D.S. o ai suoi delegati.
<b>I dati sono esatti e aggiornati?</b>	I dati vengono tenuti esatti e aggiornati per tutta la durata del trattamento, essendo quelli derivanti dagli archivi scolastici. In caso di episodi rilevati di cyberbullismo, verranno verificate le fonti di provenienza di eventuali prove documentali relative agli stessi.
<b>Periodo di conservazione dei dati</b>	Per le finalità di prevenzione , i dati vengono conservati seguendo le indicazioni dell 'archivio di stato, relativamente alle attività di istruzione e formazione (illimitato). Per le attività di contrasto e gestione degli atti di cyberbullismo, gli eventuali dati acquisiti vengono conservati dalla scuola per il tempo necessario a svolgere le attività previste dalla normativa di riferimento.

## 10 Misure a tutela dei diritti degli interessati

<b>Come sono informati del trattamento gli interessati?</b>	Gli interessati vengono informati del trattamento tramite apposita informativa fornita dalla scuola
<b>Quando applicabile: come si ottiene il consenso degli interessati?</b>	Non è richiesto il consenso degli interessati
<b>Esercizio dei diritti degli interessati</b>	E' messo a disposizione degli interessati un modulo di esercizio dei propri diritti pubblicato anche nel sito web istituzionale. Gli interessati possono sempre rivolgersi all 'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.
<b>Esercizio del Diritto all' oblio</b>	E' messo a disposizione degli interessati un modulo di esercizio dei propri diritti pubblicato anche nel sito web istituzionale. Gli interessati possono sempre rivolgersi all 'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.
<b>Esercizio diritto di limitazione e di opposizione</b>	E' messo a disposizione degli interessati un modulo di esercizio dei propri diritti pubblicato anche nel sito web istituzionale . Gli interessati possono sempre rivolgersi all 'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.
<b>Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?</b>	Il gestore del servizio cloud di segreteria digitale è stato nominato Responsabile de l Trattamento ai sensi degli Art. 28 del Reg. UE 679/2016. La piattaforma di didattica a distanza è stata

	nominata Responsabile del Trattamento ai sensi degli Artt. 28 del Reg. UE 679/2016.
<b>Garanzie per il trasferimento di dati al di fuori dell'Unione europea</b>	Non sono previsti trasferimenti di dati al di fuori dell'U.E.

## 11 Rischi Misure esistenti o pianificate

<b>Controllo degli accessi logici</b>	L'accesso alle funzionalità del sistema di segreteria digitale è regolato da un sistema di attivazione di account con permessi specifici, protetti da password, attivabili e disattivabili dall'amministratore del software (il D.S. o un suo delegato).
<b>Crittografia</b>	I dati sono trattati tramite l'utilizzo di meccanismi di conservazione e comunicazione cifrati, ai fini di garantire la minimizzazione del rischio di accesso agli stessi.
<b>Antivirus/malware</b>	I sistemi scolastici sono protetti da malware con modalità di protezione sia hardware che software (firewall e antivirus).
<b>Backup</b>	I sistemi di segreteria digitale utilizzati per il trattamento sono provvisti di una modalità di backup.
<b>Archiviazione</b>	Tutta la documentazione relativa all'attività Istituzionale dell'Amministrazione è regolata dalla normativa vigente in materia di archiviazione nella pubblica amministrazione, contenente indicazioni specifiche per la pubblica istruzione.
<b>Minimizzazione dei dati</b>	I dati vengono trattati e archiviati in forma minima, per quanto previsto dalla normativa vigente
<b>Manutenzione</b>	Viene effettuata regolarmente una attività di manutenzione nei confronti dei sistemi hardware scolastici. Il responsabile del trattamento garantisce inoltre il corretto funzionamento del software di segreteria.
<b>Contratto con il responsabile del trattamento</b>	Il responsabile del trattamento è stato nominato tale tramite la stipula di un contratto, ai sensi degli Art. 28 del Reg. Ue 679/2016
<b>Sicurezza dei canali informatici</b>	I canali interni della scuola sono protetti da firewall. Tutti i protocolli di comunicazione utilizzati dal software di segreteria digitale sono cifrati.
<b>Sicurezza dell'hardware</b>	Le postazioni hardware sono conservate all'interno di locali che vengono chiusi a chiave durante i periodi di chiusura della scuola, protetti tramite sistema di allarme. Durante i periodi di apertura al pubblico della scuola, viene garantita la custodia degli stessi tramite

	istruzioni scritte al personale interessato.
<b>Politica di tutela della privacy</b>	L'amministrazione ha messo in atto una serie di misure orientate all'adeguamento della stessa alla normativa vigente.
<b>Gestire gli incidenti di sicurezza e le violazioni dei dati personali</b>	L'amministrazione ha emesso un regolamento interno per la gestione dei data breach , al cui interno sono specificate le modalità di gestione di tali fenomeni.

## 12 Accesso illegittimo ai dati

<b>Impatti sugli interessati se il rischio si dovesse concretizzare</b>	Per le attività di prevenzione , non si ravvedono particolari impatti sugli interessati ., Per le attività di intervento e gestione degli atti di cyberbullismo, è possibile che vengano rese pubbliche le prove degli atti , il che potrebbe portare ad una limitazione dei diritti e delle libertà degli interessati.
<b>Principali minacce</b>	Accesso illecito ai dati, Pubblicazione dei dati
<b>Fonti di rischio</b>	Errore umano , Mancato inserimento dei dati all'interno di una modalità di conservazione riservata
<b>Misure pianificate per la mitigazione del rischio</b>	Crittografia, Controllo degli accessi logici, Minimizzazione dei dati, Lotta contro il malware, Backup, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Sicurezza dell'hardware, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali
<b>Stima della gravità del rischio alla luce degli impatti potenziali e delle misure pianificate</b>	<p>Importante, Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare , ma con difficoltà reali e significative :</p> <p>- psicologici: grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie psicologiche, ecc.</p> <p>In particolare, l'accesso e la potenziale pubblicazione dei dati comprovanti l'atto di cyberbullismo potrebbe comportare un aggravamento o una mala gestione del problema.</p>
<b>Probabilità del rischio con riguardo alle minacce, alle fonti di rischio e alle misure pianificate</b>	Trascurabile, Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti (ad esempio: accesso e copia di un documento

	comprovante atti di cyberbullismo, conservato con modalità che permettano l'accesso al solo D.S.)
--	---

### 13 Modifiche indesiderate dei dati

<b>Impatti sugli interessati se il rischio si dovesse concretizzare</b>	Potrebbe limitare le possibilità di intervento dell'amministrazione o dell'autorità giudiziaria.
<b>Principali minacce</b>	Accesso illecito ai dati e modifica degli stessi
<b>Fonti di rischio</b>	Errore umano, Fonti umane interne, che intervengano nella modifica dei dati
<b>Misure pianificate per la mitigazione del rischio</b>	Crittografia, Controllo degli accessi logici, Archiviazione, Minimizzazione dei dati, Backup, Lotta contro il malware, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Sicurezza dell'hardware, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali
<b>Stima della gravità del rischio alla luce degli impatti potenziali e delle misure pianificate</b>	<p>Importante, Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative :</p> <p>- psicologici: grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie psicologiche, ecc.</p> <p>In particolare, la modifica dei dati comprovanti l'atto di cyberbullismo potrebbe comportare un aggravamento o una mala gestione del problema.</p>
<b>Probabilità del rischio con riguardo alle minacce, alle fonti di rischio e alle misure pianificate</b>	Trascurabile, Le modalità di protezione dei dati rendono improbabile una azione del genere . L'esistenza di un backup e del tracciamento delle attività, inoltre, rende possibile il recupero delle informazioni originali e l'identificazione delle fonti di modifica dei dati stessi.

### 14 Perdita di dati

<b>Impatti sugli interessati se il rischio si dovesse concretizzare</b>	Perdita dei dati relativi ad atti di cyberbullismo, che essi possano costituire o no reato
<b>Principali minacce</b>	Distruzione dei server di segreteria digitale, Perdita dell'accesso ai documenti
<b>Fonti di rischio</b>	Fonti umane interne, Fonti umane esterne (incaricati del responsabile del trattamento o dei

	sub- responsabili), Eventi naturali che possano influire sui dispositivi fisici di archiviazione.
<b>Misure pianificate per la mitigazione del rischio</b>	Crittografia, Controllo degli accessi logici, Contratto con il responsabile del trattamento, Archiviazione, Minimizzazione dei dati, Lotta contro il malware, Backup, Sicurezza dei canali informatici, Manutenzione, Sicurezza dell'hardware, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali
<b>Stima della gravità del rischio alla luce degli impatti potenziali e delle misure pianificate</b>	<p>Importante, Gli interessati potrebbero subire conseguenze significative , che dovrebbero essere in grado di superare , ma con difficoltà reali e significative :</p> <p>- psicologici: grave disturbo psicologico (depressione, fobie), senso di violazione della privacy e di un danno irreparabile, esposizione a ricatti, cyberbullismo e molestie psicologiche, ecc.</p> <p>In particolare, la perdita dei dati comprovanti l'atto di cyberbullismo potrebbe comportare un aggravamento o una mala gestione del problema.</p>
Probabilità del rischio con riguardo alle minacce, alle fonti di rischio e alle misure pianificate	Trascurabile, Le modalità di protezione dei dati rendono improbabile una azione del genere . L'esistenza di un backup e del tracciamento delle attività, inoltre, rende possibile il recupero delle informazioni originali e l'identificazione delle fonti di modifica dei dati stessi.

