DIREZIONE DIDATTICA STATALE
2° CIRCOLO "E.Celentano" – POMPEI -
Via Civita Giuliana n. 26 - ☎ 081/8506209 - telefax 081/8506929
Codice Scuola : NAEE220002 - C.F. 82015230632
Indirizzo e-mail Posta ordinaria: naee220002@istruzione.it Posta PEC: naee220002@pec.istruzione.it
Sito WEB: www.pompeisecondocircolo.edu.it Codice univoco IPA: UFJ5EW

Prot. 6562 /A39 Pompei, 12/10/2021

Informazioni sulla PIA

Nome della PIA
Cyberbullismo

Nome autore
Ing. Luciano Bernardo

Nome validatore
Ing. Antonio Bove

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

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.

Quali sono le responsabilità connesse al trattamento?

Il titolare del trattamento è l'amministrazione scolastica nella persona del Dirigente Scolastico.
I dati potrebbero essere condivisi con l'autorità giudiziaria, su richiesta esplicita della stessa. I dati relativi essere condivisi anche 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.

Ci sono standard applicabili al trattamento?

Non sono stati definiti degli standard applicabili a questo tipo di trattamento.

Valutazione: Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Dati anagrafici di alunni, genitori e dipendenti della scuola. Eventuali dati personali degli esperti esterni che prestano attività formativa e informativa.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

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 o di un suo eventuale delegato.

I dati degli esperti esterni incaricati delle attività formative e informative vengono trattai secondo le modalità descritte nel registro dei trattamenti, relative al trattamento di dati personali di esperti esterni alla scuola.

Quali sono le risorse di supporto ai dati?

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, il software utilizzato consiste nel gestionale per la segreteria digitale. 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.

Valutazione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

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.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

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.

Valutazione: Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

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.

Valutazione: Accettabile

I dati sono esatti e aggiornati?

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.

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

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 constrasto 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.

Valutazione: Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati vengono informati del trattamento tramite apposita informativa fornita dalla scuola.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Per questa tipologia di trattamento non è previsto il consenso da parte dell'interessato.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

La scuola mette a disposizione degli interessati un modulo per esercitare i propri diritti.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

La scuola mette a disposizione degli interessati un modulo per esercitare i propri diritti.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

La scuola mette a disposizione degli interessati un modulo per esercitare i propri diritti.

Valutazione: Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Il gestore del servizio in cloud di segreteria digitale è stato nominato Responsabile del Trattamento ai sensi degli Artt. 28 e 29 del Reg. UE 679/2016 ed è vincolato da un contratto di prestazioni del servizio.

Valutazione: Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

Qualora i gestori dei servizi di segreteria in cloud dovessero trasferire i dati fuori dall Unione Europea, questi potranno essere trasferiti negli USA, nella misura in cui il gestore della piattaforma abbia adottato meccanismi di garanzia come ad esempio le BCR – Binding Corporate Rules (Norme Vincolanti di Impresa) oppure abbia aderito a specifici protocolli (es. Privacy Shield) in quanto società operanti nel territorio della Comunità Europea sono vincolati alle disposizioni obbligatorie indicate nel Regolamento UE 679/16 in materia di Protezione dei Dati Personali.

Valutazione: Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

I dati sono trattati tramite l'utilizzo di meccanismi di conservazione e comunicazione cifrati, ai fini di garantire la minimizzazione del rischio di acceso agli stessi.

Valutazione: Accettabile

Controllo degli accessi logici

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 su indicazione del Titolare.

Valutazione: Accettabile

Archiviazione

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.

Valutazione: Accettabile

Minimizzazione dei dati

I dati vengono trattati e archiviati in forma minima, così come previsto dalla normativa vigente

Valutazione: Accettabile

Lotta contro il malware

I sistemi scolastici sono protetti da malware con modalità di protezione sia hardware che software (firewall e antivirus).

Valutazione: Accettabile

Backup

I sistemi di segreteria digitale utilizzati per il trattamento sono provvisti di funzioni di backup automatico.

Valutazione: Accettabile

Manutenzione

Il responsabile del trattamento garantisce una regolare attività di manutenzione dei sistemi hardware scolastici ed il corretto funzionamento del software di segreteria.

Valutazione: Accettabile

Contratto con il responsabile del trattamento

Il responsabile del trattamento è stato nominato tale tramite la stipula di un contratto, ai sensi degli Artt. 28 e 29 del Reg. Ue 679/2016

Valutazione: Accettabile

Sicurezza dei canali informatici

Tutti i protocolli di comunicazione utilizzati dal software di segreteria digitale sono cifrati.

Valutazione: Accettabile

Sicurezza dell'hardware

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.

Valutazione: Accettabile

Politica di tutela della privacy

L'amministrazione ha messo in atto una serie di misure orientate all'adeguamento della stessa alla normativa vigente.

Valutazione: Accettabile

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

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.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso illecito ai dati, diffusione dei dati.

Quali sono le fonti di rischio?

Errore umano, mancata conservazione dei dati in modalità riservata.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Sicurezza dei canali informatici, Sicurezza dell'hardware, Politica di tutela della privacy, Crittografia, Controllo degli accessi logici, Archiviazione, Minimizzazione dei dati, Lotta contro il malware, Backup, Manutenzione, Contratto con il responsabile del trattamento

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante, Gli interessati potrebbero subire conseguenze anche gravi.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, Appare improbabile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti

Valutazione: Accettabile

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Potrebbe limitare le possibilità di intervento dell'amministrazione o dell'autorità giudiziaria.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Accesso illecito ai dati e modifica degli stessi

Quali sono le fonti di rischio?

Errore umano da parte di fonti interne o acesso abusivo da parte di fonti esterne.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Archiviazione, 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

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Importante, Gli interessati potrebbero subire conseguenze anche gravi di carattere psicologico.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e 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 finti di modifica dei dati stessi.

Valutazione: Accettabile

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Perdita dei dati relativi ad atti che potrebbero essere utilizzati come prove di cyberbullismo.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Distruzione dei server di segreteria digitale, Perdita dell'accesso ai documenti

Quali sono le fonti di rischio?

Fonti umane interne o esterne (incaricati del responsabile del trattamento o dei sub-responsabili), Eventi naturali che possano influire sui dispositivi fisici di archiviazione.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Minimizzazione dei dati, Crittografia, Controllo degli accessi logici, Archiviazione, Lotta contro il malware, Backup, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Sicurezza dell'hardware, Politica di tutela della privacy

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante, Gli interessati potrebbero subire conseguenze psicologiche significative

Come stimereste la probabilità del rischio, specialmente 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.

Valutazione: Accettabile

Piano d'azione

Panoramica

Principi fondamentali

Nessun piano d'azione registrato.

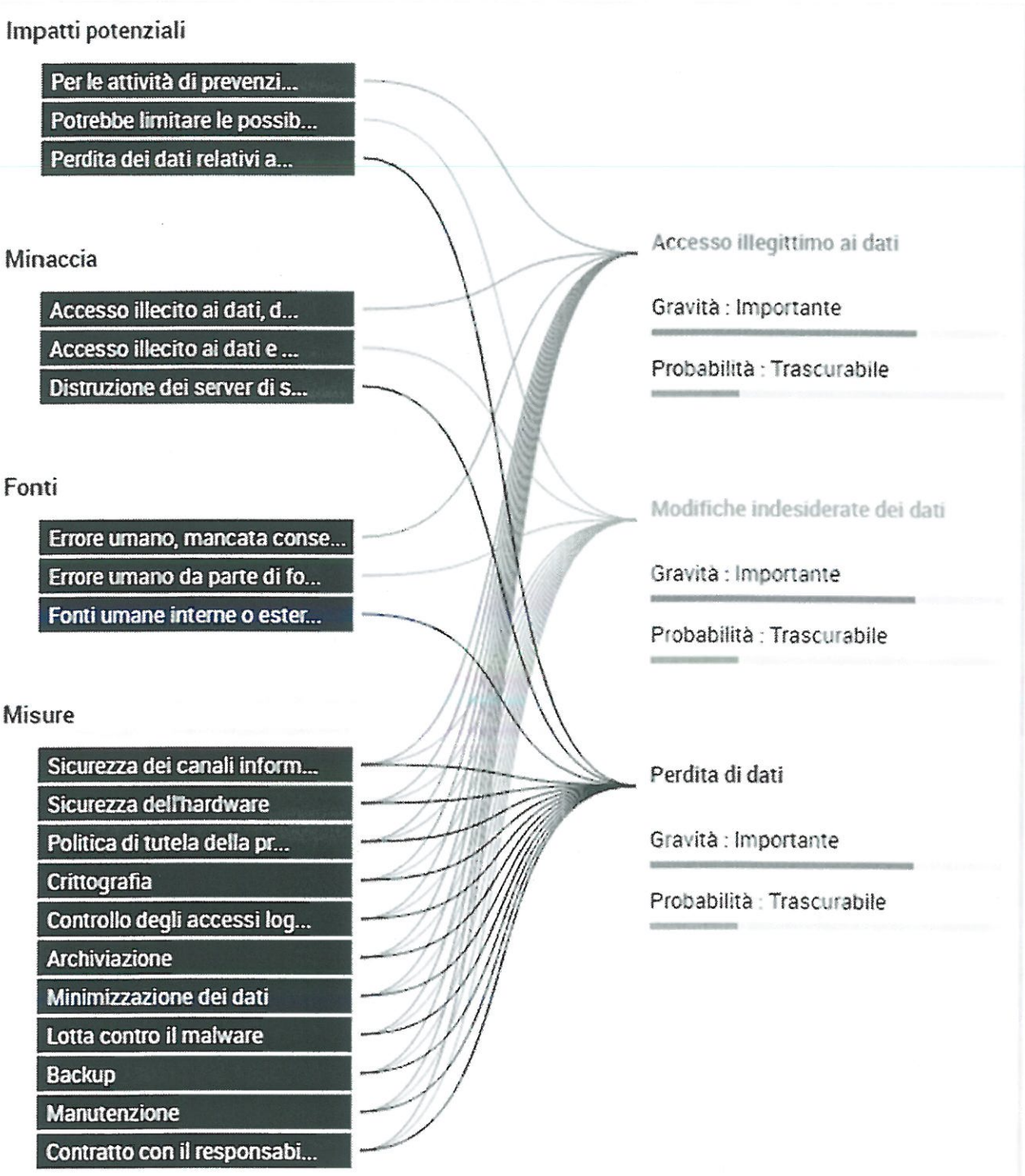
Misure esistenti o pianificate

Nessun piano d'azione registrato.

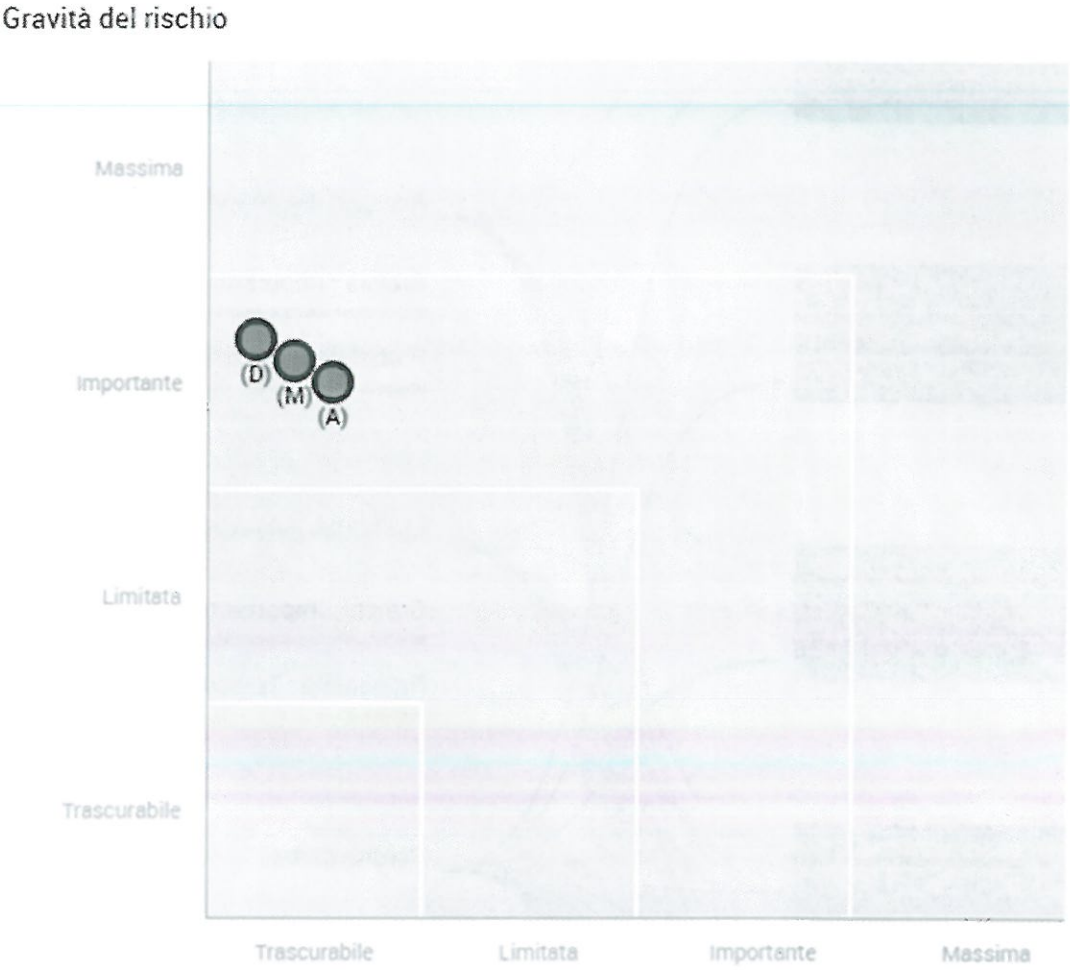
Rischi

Nessun piano d'azione registrato.

Panoramica dei Rischi



Mappaggio dei Rischi



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati