CENTRO PROVINCIALE PER L'ISTRUZIONE DEGLI ADULTI 2 NORD EST MILANO

PIAZZA A. COSTA, 23 CINISELLO BALSAMO (MI)

Modello Organizzativo sul Trattamento dei Dati Regolamento Europeo Privacy 2016/679

SOMMARIO

ATTENZIONE! Prima di utilizzare il presente documento verificare che sia in ultima edizione

Revisioni e/o aggiornamenti

Ed.	Data	Descrizione revisione e/o aggiornamento
02	13 Settembre 2019	Redatto Modello Organizzativo sul trattamento dei dati personali in ottemperanza al Regolamento Europeo 2016/679
03	12 novembre 2020	Aggiornamento Modello Organizzativo sul trattamento dei dati personali in ottemperanza al Regolamento Europeo 2016/679

1 SCOPO

1.1 Premessa

Il presente documento è stato redatto in conformità al Regolamento Generale dell'Unione Europea sulla protezione dei dati, 27 Aprile 2016, n. 679 (GDPR 2016/679), al fine di individuare, analizzare ed applicare un complesso di contromisure per garantire la massima sicurezza in ordine al trattamento dei dati personali.
Tale documento viene aggiornato con frequenza annuale.
Il Centro Provinciale per l'Istruzione degli Adulti 2 (di seguito solo CPIA 2) effettua un'attività di istruzione degli allievi iscritti presso la stessa.

1.2 Finalità

Il presente documento ha lo scopo di:

- Definire e riportare sotto il profilo normativo gli obblighi che il CPIA 2 deve adempiere in merito all'adozione delle misure adeguate di sicurezza.
- Tutelare gli interessi dei soggetti pubblici e privati che fanno affidamento sui trattamenti di dati personali svolti dalla scuola.
- Evitare eventi pregiudizievoli che possono danneggiare disponibilità, riservatezza e integrità del patrimonio dati personali trattati dal CPIA 2.
- Potenziare la consapevolezza dei rischi e delle insidie che possono coinvolgere il trattamento dei dati personali effettuato con l'ausilio di sistemi informativi automatizzati o tramite supporto cartaceo.
- Definire le soluzioni logiche, fisiche e organizzative al fine di prevenire situazioni di pericolo.
- Individuare le misure di sicurezza e le procedure per ridurre al minimo la distruzione o la perdita dei dati, l'accesso non autorizzato ed il trattamento non consentito o non conforme.

2 PRINCIPI GENERALI APPICABILI AL TRATTAMENTO DEI DATI PERSONALI

Si riportano i principi generali alla base del trattamento dei dati personali, adottati dal CPIA 2.
I dati personali sono:

a) Trattati in modo lecito, corretto e trasparente nei confronti dell'interessato: principio di "*liceità*, *correttezza* e *trasparenza*".

b) Raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali principio di "*limitazione della finalità*".

c) Adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati: principio di "*minimizzazione dei dati*".

d) Esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati: principio di "*esattezza*".

e) Conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato: principio di "*limitazione della conservazione*".

f) Trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali: principio di "*integrità e riservatezza*".

2.1 Il principio di "Accountability" - Responsabilizzazione

Il CPIA 2, in qualità di Titolare del trattamento, si impegna ad adottare politiche ed attuare misure adeguate al fine di garantire ed essere in grado di dimostrare che il trattamento dei dati personali effettuato è conforme alle disposizioni del GDPR 2016/679.

3 CAMPO DI APPLICAZIONE

Il presente documento definisce le politiche e gli standard di sicurezza in merito al trattamento, interamente o parzialmente automatizzato, di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi, in particolare:

- l'analisi dei trattamenti di dati personali;
- la distribuzione dei compiti e delle responsabilità;
- l'analisi dei rischi che incombono sui dati in termini di impatto;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità di ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento;
- la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati;
- la definizione di idonee misure di sicurezza in caso di trattamenti effettuati da parte di soggetti esterni.

4 RIFERIMENTI NORMATIVI

- D.Lgs. 196 del 30 giugno 2003 "*Codice in materia di Protezione dei dati personali – Legge delega n. 127/2001*" come novellato dal D.lgs 101 del 10 agosto 2018 "*Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, del 27 aprile 2016"*.
- Provvedimento del Garante del 27 novembre 2008 "*Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema*".
- Provvedimento del Garante del 13 ottobre 2008 "*Rifiuti di apparecchiature elettriche ed elettroniche (Raae) e misure di sicurezza dei dati personali*".
- Decreto Legge 6/12/2011 n. 201 che all'art. 4 modifica l'ambito di applicazione del Codice Privacy, ora allineato a quanto previsto dalla normativa europea.
- D.Lgs. 28 maggio 2012, n. 69 in attuazione alla delega prevista nell'art. 9 della Legge comunitaria del 2010 (L. n. 217/2011) per il recepimento della direttiva 2009/136/CE in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche.
- Provvedimento del Garante 08/05/2014 n° 229 "*Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookie*".
- Regolamento Europeo in materia di Protezione dei Dati Personali 2016/679.
- DPCM 11 marzo 2020, in particolare Protocollo Condiviso 14 marzo 2020, Protocollo 24 aprile 2020 e successive integrazione e modificazioni nell'ambito dell'emergenza COVID

4.1 Altri Riferimenti

- D.Lgs. 30 marzo 2001, n. 165 "*Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche*";
- CCNL vigente;
- D.Lgs. 16 aprile 1994, n. 297 "*Testo Unico delle disposizioni legislative vigenti in materia*

di istruzione, relative alle scuole di ogni ordine e grado";

- Legge 3 maggio 1999, n. 124 "*Disposizioni urgenti in materia di personale scolastico*";
- Legge 12 giugno 1990, n. 146 "*Norme sull'esercizio del diritto di sciopero nei servizi pubblici essenziali e sulla salvaguardia dei diritti della persona costituzionalmente tutelati. Istituzione della Commissione di garanzia dell'attuazione della legge*";
- D.I. 1 febbraio 2001, n. 44 "*Regolamento concernente le istruzioni generali sulla gestione amministrativo-contabile delle istituzioni scolastiche*";
- D.P.R. 22 giugno 2009, n. 119 "*Regolamento recante disposizioni per la definizione dei criteri e dei parametri per la determinazione della consistenza complessiva degli organici del personale amministrativo tecnico ed ausiliario (ATA) delle istituzioni scolastiche ed educative statali, a norma dell'articolo 64, commi 2, 3 e 4 lettera e) del decreto-legge 25 giugno 2008, n. 112, convertito, con modificazioni, dalla legge 6 agosto 2008, n. 133*";
- D. Lgs. 18 aprile 2016, n. 50 "*Codice dei contratti pubblici*";
- D.P.R. 5 gennaio 1950, n. 180 "*Approvazione del testo unico delle leggi concernenti il sequestro, il pignoramento e la cessione degli stipendi, salari e pensioni dei dipendenti dalle Pubbliche Amministrazioni*";
- D.M. 7 dicembre 2006, n. 305 "*Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della pubblica istruzione, in attuazione degli articoli 20 e 21 del decreto legislativo 30 giugno 2003, n. 196, recante «Codice in materia di protezione dei dati personali»*".

4.2 Riferimenti bibliografici

- ENISA "Handbook on Security of Personal Data Processing"
- CNIL-PIA Methodology
- Metodologia VERA Privacy – Cesare Gallotti

5 DEFINIZIONI

a) **"Trattamento"**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insieme 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.

b) **"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.

c) **"Limitazione di trattamento":** il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

d) **"Profilazione":** qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di 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.

e) **"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 organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile.

f) **"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.

g) **"Titolare del trattamento":** la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali. Quando le finalità e i mezzi di tale trattamento sono determinati 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.

h) **"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.

i) **"Destinatario":** la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di tali dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una 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.

j) **"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.

k) **"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.

l) **"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.

m) **"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.

n) **"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.

o) **"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.

p) **"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 abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che 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.

q) **"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.

r) **"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.

s) **"Gruppo imprenditoriale":** un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate.

t) **"Norme vincolanti d'impresa":** le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio 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.

u) **"Autorità di controllo":** l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51.

v) **"Autorità di controllo interessata":** un'autorità di controllo interessata dal trattamento di dati personali in quanto:

- Il Titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo.
- Gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure
- Un reclamo è stato proposto a tale autorità di controllo.

w) **"Trattamento Transfrontaliero"**: a) Trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro, oppure; b) Trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro.

x) **"Obiezione pertinente e motivata"**: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione.

y) **"Servizio della società dell'informazione"**: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio.

z) **"Organizzazione internazionale"**: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

aa) **"Interessato"**: La definizione di "interessato", non essendocene una diretta, è desumibile dall'articolo 5, comma 1 che, definendo il "dato personale" dispone che: "*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*".

6 ANALISI DEL CONTESTO IN CUI OPERA LA SCUOLA E PARTI INTERESSATE

Il CPIA 2 è situato in Cinisello Balsamo (MI), Piazza Andrea Costa 23.
È suddivisa in n. 3 plessi, così dislocati:

a) Sede amministrativa del CPIA2 Milano e sede associata di Cinisello Balsamo, sita in Piazza A. Costa, 23;
b) Sede associata di Pioltello, sita in Via Bizet, 3/a;
c) Sede associata di Sesto San Giovanni, sita in Via Saint Denis, 200.

6.1 Descrizione del flusso di gestione dei dati

I luoghi del CPIA 2 sono ospitati presso gli Istituti Comprensivi del territorio.
CPIA 2 tratta prevalentemente i dati comuni sia per il personale lavoratore (corpo docente e personale di segreteria), che per gli studenti iscritti.
Inoltre, per il personale lavoratore il CPIA 2 tratta i dati relativi a eventuali condanne penali o carichi pendenti ex art. 10 del Regolamento UE 2016/679.
Tutti i dati sono trattati sia in modo cartaceo che in modo digitale.
I dati degli studenti sono raccolti al momento dell'iscrizione online attraverso il link di collegamento direttamente al registro elettronico (SOGI) presente sul sito web del Centro di Formazione.
Il trattamento dei dati eseguito da CPIA 2 è analiticamente riportato nel Registro dei trattamenti semplificato nel presente documento.

Emergenza Covid 19

Nell'ambito dell'emergenza COVID19 l'Istituto ha applicato un protocollo sulla salute e sicurezza che prevede misure organizzative e di protezione dei dipendenti, relativamente a:

- informazione ai lavoratori sulle condizioni che precludono l'accesso all'Istituto (al fine di minimizzare il rischio di contagio e il trattamento dei dati personali)
- modalità di accesso agli uffici
- utilizzo di procedure dedicate per la pulizia e la sanificazione dei locali
- adozione di DPI e procedure per il personale che accede agli uffici
- organizzazione del lavoro, inclusa la gestione degli spazi comuni
- gestione delle persone sintomatiche
- gestione di eventuali lavoratori fragili, a cura del Medico Competente

Ulteriormente, per i dipendenti e collaboratori sarà effettuata la rilevazione in tempo reale della temperatura prima dell'accesso e per i lavoratori positivi al COVID-19, ci sarà l'eventuale acquisizione da parte dell'Istituto, della certificazione medica da cui risulti la "avvenuta negativizzazione" del tampone secondo le modalità previste e rilasciata dal dipartimento di prevenzione territoriale di competenza.
Per gli studenti saranno acquisiti dati sanitari relativi ad una particolare situazione di fragilità e per gli studenti risultati positivi al COVID-19, ai fini del rientro a scuola, certificazione medica o autocertificazione da cui risulti la "avvenuta negativizzazione" del tampone secondo le modalità previste e rilasciata dal dipartimento di prevenzione territoriale di competenza.
Per i visitatori l'Istituto effettuerà la rilevazione in tempo reale della temperatura prima dell'accesso ai locali dell'Istituto e la registrazione dei dati anagrafici (nome, cognome, data di nascita, luogo di residenza), dei relativi recapiti telefonici, nonché della data di accesso e del tempo di permanenza nell'Istituto

6.2 Infrastruttura HW – SW

Infrastruttura informatica

Il sistema informativo di CPIA 2 è costituito dalla presenza di computer client in rete tra di loro protetti da una password associata a ciascun utente.
La struttura hardware di CPIA 2 è così composta:

NOME HARDWARE	NUMERO	UTILIZZATORI
Computer fissi	8	Segreteria
Laboratori informatici	30	Docenti e alunni
Computer portatili	40	Docenti e alunni

Per quanto concerne i software è il Titolare del trattamento che definisce i software standard da installare.

È vietato, per l'utente, installare software di qualsiasi tipo, scaricato da Internet, giochi, screen saver o qualsiasi altra utility non preventivamente autorizzata dal Centro di Formazione. È necessario attenersi ai software ufficiali per evitare i rischi di infezione da virus e problemi di conflitto tra software. Si riporta la configurazione software di base dei pc.

NOME SOFTWARE	DESCRIZIONE	UTILIZZATORI
Windows 7 Pro, 8.1, 10	Sistema Operativo	Segreteria
Microsoft Office	Suite office automation	Segreteria
Kaspersky	Antivirus	Segreteria
Sogi	Registro elettronico	Segreteria – famiglie - docenti

6.3 Sito internet

Lo scopo del sito web scolastico istituzionale

CPIA 2 cpia2milano.edu.it è quello di aprire un canale di comunicazione diretta tra l'Istituto e gli studenti.
Infatti, sul sito web sono pubblicate tutte le comunicazioni e le circolari di pubblico interesse, nonché tutti i dati di contatto o di riferimento dei vari responsabili di funzione.
La cura e la gestione del sito internet è affidata a GiEffe Informatica di Giovanni Franco.
Il sito web è stato creato grazie al progetto "Porte aperte sul web" e l'hosting del dominio è presso Aruba S.p.A. (con data center all'interno dell'UE).

6.4 Videosorveglianza

Il CPIA 2 non è dotato di alcun impianto di videosorveglianza.

7 ANALISI DEI DATI PERSONALI TRATTATI

Il CPIA 2 tratta i dati personali per i seguenti scopi:

a) gestione ed organizzazione della composizione delle classi di studenti;
b) organizzazione del corpo docente (organizzazione degli orari di lezione e/o supplenza, comunicazione con i docenti e/o le loro rappresentanze sindacali);
c) organizzazione del personale ATA (organizzazione degli orari pomeridiani per attività scolastiche e/o extrascolastiche);
d) gestione ed organizzazione degli organi collegiali e delle loro adunanze.

7.1 Categorie dei dati personali trattati e di interessati

La natura dei dati trattati è stata classificata sulla base di quanto previsto dal Regolamento Europeo 2016/679. Nello specifico, si è proceduto alla verifica ed alla successiva categorizzazione dei dati per tipologia. In particolare i dati più rilevanti trattati dal Titolare del trattamento sono:

a) Dati personali che si riferiscono a persone fisiche nell'ambito dei rapporti tra CPIA 2 e gli studenti, i docenti, il personale ATA.
b) Dati personali relativi ad altri soggetti (candidati all'assunzione, consulenti e professionisti, agenti nel caso in cui il trattamento riguardi dati ulteriori rispetto a quelli meramente scolastici).
c) Dati relativi allo svolgimento di attività marketing e promozione delle attività scolastiche.
d) Dati relativi alle Risorse Umane, di natura potenzialmente anche sensibile. A tal proposito si segnala che il Titolare del trattamento, al quale sono fornite informazioni di carattere personale strettamente indispensabili per dare esecuzione al rapporto di lavoro, individua il personale che può trattare tali dati e assicura idonee misure di sicurezza per proteggerli da indebite intrusioni o illecite divulgazioni.
e) Dati giudiziari.

Si riporta la sintesi delle categorie di dati personali trattati da CPIA 2.

Tipologia	Descrizione	Applicato
Identificativi	- Nome, Cognome, sesso	☑
Altri dati identificativi	- Età, luogo e data di nascita, indirizzo privato, numero di telefono privato, email personale. - Numero di carta identità/numero di passaporto - Dati fisici (altezza, peso) - Auto aziendale (modello e targa) - Codice fiscale - Carte sanitarie - Stato civile, figli, soggetti a carico, appartenenti al nucleo familiare	☑ ☑ ☐ ☐ ☑ ☑ ☑
Immagini	- Immagini e filmati - Immagini o suoni raccolti dall'impianto di videosorveglianza	☐ ☐
Dati sensibili	- Dati idonei a rilevare lo stato di salute - Dati idonei a rivelare lo stato di gravidanza. - Dati idonei a rivelare l'appartenenza a categorie protette. - Dati idonei a rivelare lo stato di disabilità. - Origini razziali o etniche - Appartenenza religiosa - Appartenenza ad associazioni sindacali - Giudizi di idoneità alla mansione in caso di restrizioni - Infortuni, informazioni raccolte nell'ambito di quanto definito dalla normativa in materia di Salute e Sicurezza sul lavoro	☑ ☑ ☑ ☑ ☑ ☐ ☐ ☑ ☑
Dati giudiziari	- Carichi pendenti - Casellario giudiziale	☑ ☑
Istruzione e cultura	- Curriculum di studi e/o accademico. - Titoli di studio - Pubblicazioni e lavori attribuibili all'interessato	☑ ☑ ☑
Esperienze Lavoro	- Occupazione attuale e precedente. - Informazioni sul tirocinio o sulla formazione professionale. - Dati relativi alle pregresse esperienze professionali. - Retribuzioni, assegni, integrazioni salariali e trattenute.	☑ ☑ ☑ ☐
Dati commerciali e finanziari	- Dati contabili - Ordini, fatture, contratti - Transazioni - Identificativi finanziari - Dati finanziari relativi a investimenti, passività, solvibilità, prestiti, mutui, ipoteche, crediti, indennità, benefici, concessioni, donazioni, sussidi, contributi - Dati assicurativi - Dati previdenziali	☐ ☐ ☐ ☐ ☐ ☑ ☑
Profilazione	- Acquisti effettuati, servizi ricevuti, preferenze espresse, cookies - Carte fedeltà	☐ ☐
Dati di navigazione	- Profili utenti (dati di navigazione) Preferenze di navigazione	☑ ☐
Geolocalizzazione e controllo accessi	- Strumenti di rilevazione presenze (es. registrazione di ingressi o uscite presso luoghi di lavoro tramite badge o codici personali) - Geolocalizzazione di veicoli - Geolocalizzazione effettuata attraverso dispositivi mobili	☐ ☐ ☐
Dati biometrici	- Dati identificativi per rilevazione presenze o gestione accessi ai luoghi aziendali	☐
Abitudini di vita e consumo	- Viaggi, spostamenti, preferenze o esigenze alimentari - ad eccezione di quelle fondate su convinzioni religiose o filosofiche - Dati relativi all'appartenenza ad associazioni diverse da quelle di carattere religioso, filosofico, politico o sindacale, (es. licenze, autorizzazioni, dati relativi ad attività sportive o agonistiche)	☐ ☐

Il dettaglio dei trattamenti è riportato nella sintesi delle banche dati riportata di seguito.

7.2 Individuazione delle banche dati e interessati al trattamento

Si riporta l'elenco delle banche dati sono riportate di seguito, specificando se si tratta di dati sensibili, personali, giudiziari. L'accesso alle banche dati avviene tramite computer fissi, server e archivio cartaceo.

Finalità del trattamento o attività svolta **Interessati: DOCENTI / PERSONALE ATA**	**Tipologia trattamento**	**Base giuridica trattamento**	**Soggetti incaricati**	**Soggetti esterni che effettuano il trattamento**	**Tempo di conservazione**	**Strumenti e banche dati utilizzati**
Gestione anagrafica di implementazione Elaborazione cedolini paga per compensi accessori Gestione del personale per supplenze per brevi e medi periodi Gestione delle presenze dei lavoratori	Dati anagrafici Dati identificativi Coordinate bancarie Nucleo familiare Numero di protocollo del certificato di malattia	Obblighi di legge del Titolare	Segreteria	MIUR MEF – Ragioneria territoriale MEF – "NoiPA"	Permanente. In caso di trasferimento del lavoratore, il fascicolo personale viene trasferito alla scuola di destinazione	Digitale: Server Cartaceo: fascicoli personali dei lavoratori archiviati in segreteria
Autodichiarazione di eventuali carichi pendenti	Condanne penali e reati	Esecuzione di un interesse pubblico	Segreteria			Cartaceo: fascicoli personali dei lavoratori archiviati in segreteria
Gestione di eventuali infortuni	Dati anagrafici Dati identificativi	Interesse legittimo del Titolare	Segreteria	MIUR		Cartaceo: fascicoli personali dei lavoratori archiviati in segreteria
Gestione della sicurezza e salute sui luoghi di lavoro	Dati anagrafici Dati identificativi Dati riferiti all'attività lavorativa Dati riferiti all'idoneità allo svolgimento della mansione Dati riferiti alla formazione obbligatoria	Obblighi di legge del Titolare	Segreteria	Consulente della sicurezza ex d.lgs 81/08		Cartaceo: fascicoli relativi alle polizze assicurative

Finalità del trattamento o attività svolta **Interessati: CANDIDATI – Messe a disposizione**	**Tipologia trattamento**	**Base giuridica trattamento**	**Soggetti incaricati**	**Soggetti esterni che effettuano il trattamento**	**Tempo di conservazione**	**Strumenti e banche dati utilizzati**
Ricerca e selezione di supplenti per brevi periodi	Dati anagrafici Dati identificativi Istruzione e cultura Esperienze di Lavoro	Interesse legittimo del Titolare del trattamento	Segreteria	MIUR	1 anno	Casella di posta elettronica
Finalità del trattamento o attività svolta **Interessati: COLLABORATORI ESTERNI**	**Tipologia trattamento**	**Base giuridica trattamento**	**Soggetti incaricati**	**Soggetti esterni che effettuano il trattamento**	**Tempo di conservazione**	**Strumenti e banche dati utilizzati**
Ricerca e selezione di eventuali professionisti esterni Elaborazione contratti di collaborazione Elaborazione Certificazione Unica	Dati anagrafici Dati identificativi Titolo di studio Esperienze di lavoro Corsi di formazione/specializzazione	Interesse legittimo del Titolare del trattamento Obblighi di legge del Titolare	Segreteria	MIUR	Permanete	Fattura elettronica: digitale e cartacea (nel faldone personale e armadio chiuso a chiave) Cartaceo allegato al mandato di assunzione e al bilancio Contratti sia digitale che cartaceo (cartaceo: nel fascicolo personale Digitale: in locale sui pc del personale di segreteria)
autodichiarazione	Dati giudiziari				Vedi sopra	Fascicolo personale
Finalità del trattamento o attività svolta **Interessati: STUDENTI**	**Tipologia trattamento**	**Base giuridica trattamento**	**Soggetti incaricati**	**Soggetti esterni che effettuano il trattamento**	**Tempo di conservazione**	**Strumenti e banche dati utilizzati**
Organizzazione classi Integrazione iscrizioni online con documentazione integrativa Gestione valutazioni ed esami	Dati anagrafici Dati identificativi Carta di identità Permesso di soggiorno Codice fiscale Situazione lavorativa Valutazioni ed esami	Obblighi di legge del Titolare	Docenti Segreteria	Sogi MIUR	Permanente	Digitale: Server Cartaceo: segreteria didattica (solo per diplomi)
Gestione di eventuali infortuni	Dati anagrafici Dati identificativi	Interesse legittimo del Titolare	Segreteria	MIUR		Cartaceo: fascicoli relativi alle polizze assicurative

Finalità del trattamento o attività svolta Interessati: GENITORI/TUTORI PER STUDEDNTI MINORI	Tipologia trattamento	Base giuridica trattamento	Soggetti incaricati	Soggetti esterni che effettuano il trattamento	Tempo di conservazione	Strumenti e banche dati utilizzati
Iscrizione Contatti per emergenze	Dati anagrafici Dati identificativi Dati di contatto	Interesse legittimo del Titolare	Segreteria	Sogi	Per il tempo di permanente o ciclo di istruzione	Digitali: server

Finalità del trattamento o attività svolta Interessati: DIPENDENTI COLLABORATORI O VISITATORI	Tipologia trattamento	Base giuridica trattamento	Soggetti incaricati	Soggetti esterni che effettuano il trattamento	Tempo di conservazione	Strumenti e banche dati utilizzati
Prevenzione dal COVID-19 Tutela della salute Collaborazione con le autorità pubbliche	Temperatura corporea senza registrazione	DPCM 11/03/20 Protocollo Condiviso 14/03/20 – 24/04/20	Incaricati all'ingresso (solo se previsto)	--	Nessuna registrazione	Termometri
	Dati identificativi del superamento soglia di 37,5°- sintomi - zone a rischio, contatti stretti	DPCM 11/03/20 Protocollo Condiviso 14/03/20 – 24/04/20	Incaricati all'ingresso (solo se previsto)	Incaricati Area Amministrazione	Solo se necessario fino al termine dell'emergenza	Comunicazione all'ufficio personale
	Stato di salute (eventuale negativizzazione del tampone)	DPCM 11/03/20 Protocollo Condiviso 14/03/20 – 24/04/20	--	Medico Competente	Fino al termine dell'emergenza o comunicazioni delle autorità	Cartella sanitaria del dipendente
	Presenza di stato di fragilità (lavoratori fragili)	DPCM 11/03/20 Protocollo Condiviso 14/03/20 – 24/04/20	--	Medico Competente	Fino al termine dell'emergenza o comunicazioni delle autorità	Cartella sanitaria del dipendente

8 INDIVIDUAZIONE FIGURE E COMPITI

8.1 Titolare del trattamento

Ai sensi del Regolamento Europeo 2016/679 si intende per titolare del trattamento "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*".

Il Titolare del trattamento deve assolvere a tutta una serie di obblighi così come previsto dall'articolo 30 del Regolamento Europeo 2016/679 a cui si rimanda.

Il Titolare del trattamento è il CPIA 2.

8.2 Responsabile del trattamento - esterno

Per responsabile del trattamento si intende "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

Il responsabile del trattamento deve presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento dei dati personali garantisca la tutela dei diritti dell'interessato.

I compiti del responsabile del trattamento sono individuati all'articolo 28 del Regolamento Europeo 2016/679.

I responsabili del trattamento esterni che trattano dati per conto di CPIA 2 sono i seguenti:

Nominativo Responsabile	Attività svolta	Tipologia di dati
Consulente della sicurezza ex d.lgs 81/08 GSI Technoprogetti s.r.l.	Consulenza ex d.lgs 81/08	Dati personali
SOGI S.n.c di Matteo Bruschetta & Nicola Pippa	Registro elettronico	Dati personali
Multimedica s.r.l.	Medicina del lavoro	Dati personali e particolari

GiEffe informatica di Giovanni Franco	Gestione sito, gestione account Microsoft 365, gestione reti	Dati personali e particolari

8.3 Responsabile della protezione dei dati (DPO)

Secondo il Regolamento Europeo 2016/679 l'istituzione del DPO è obbligatoria nei seguenti casi:

a) Il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali.

b) Le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala.

c) Le attività principali del Titolare del trattamento o del Responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Nell'articolo 4 del Regolamento UE 2016/679, che offre le definizioni, ne manca una specifica di responsabile della protezione dei dati. Il profilo è desunto dall'articolo 37, che al comma 5 dispone che "*il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e delle capacità di assolvere i compiti di cui all'articolo 39*".

L'articolo 39, per l'appunto, individua i compiti del DPO:

- Informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché alle persone autorizzate che eseguono il trattamento in merito agli obblighi derivanti dal Regolamento UE 2016/679 nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati.
- Sorvegliare l'osservanza del Regolamento UE 2016/679, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali,

  compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo.
- Fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento.
- Cooperare con l'autorità di controllo.
- Fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento.

Tutto ciò premesso, CPIA 2 ha individuato il Responsabile della Protezione dei dati personali, nominando Frareg s.r.l. e indicando quale referente l'Ing. Stéphane Jean Michel Barbosa.

8.4 Amministratore di sistema

È stato individuato la GiEffe Informatica di Giovanni Franco in qualità di Amministratore di Sistema, che sarà incaricato di espletare i seguenti compiti:

- supportare il DPO nel definire le misure di sicurezza informatica da adottare e supervisionare e/o provvedere in prima persona alla loro attuazione;
- monitorare il corretto funzionamento della rete, compresa la gestione dei filtri e del firewall;
- gestire e monitorare il sistema di back-up;
- predisporre, per ogni incaricato del trattamento, delle credenziali di accesso;
- revocare tempestivamente tutti i profili di identificazione e gli account di posta su comunicazione scritta del titolare del trattamento;
- segnalazione al Titolare del trattamento sulle non corrispondenze con le norme di sicurezza e su eventuali anomalie.

La nomina dell'amministratore di Sistema è conservata in allegato al presente documento. Sul server è presente un sistema di tracciamento che permette di memorizzare gli accessi al server. Il sistema garantisce la inalterabilità della registrazione degli accessi.

8.5 Incaricati del trattamento

Per incaricato del trattamento si intende "*la persona fisica autorizzata a compiere operazioni di trattamento dal titolare o dal responsabile*".

L'articolo 29 del Regolamento UE 2016/679 dispone che "*il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare del trattamento, che abbia accesso ai dati personali non può trattare tali dati se non è istruito in tal senso dal titolare del trattamento*".

Pertanto, al fine di svolgere le attività di trattamento dei dati personali, occorre essere espressamente autorizzati in qualità di incaricato del trattamento.

Tutto ciò comporta che, ogni persona fisica, che operi in nome e/o nell'interesse di CPIA 2 e che per questo abbia bisogno di accedere ai dati trattati dal Centro di Formazione, deve essere individuata in qualità di incaricato e conseguentemente essere autorizzata ad accedere ai dati, di cui è titolare il CPIA 2.

Il sistema di individuazione degli incaricati prevede le seguenti azioni:

- Consegna delle indicazioni operative e delle istruzioni per lo svolgimento delle operazioni e per l'accesso ai sistemi informativi e ai dati scolastici, secondo il profilo professionale di inquadramento e l'area operativa alla quale si è assegnati ovvero viene chiesto di collaborare.
- Assegnazione di credenziali di autenticazione con conseguente abilitazione all'accesso a sistemi informativi e applicativi scolastici.
- Formazione specifica sulla corretta modalità di trattamento dei dati personali.

Ciascun incaricato del trattamento individuato all'interno CPIA 2 è stato formalmente nominato da parte del titolare e/o dal responsabile. Le norme generali di comportamento sono sottoscritte a tutti gli incaricati al momento della nomina.

9 SICUREZZA DEI DATI PERSONALI

9.1 Sicurezza del trattamento

Il Titolare del trattamento e il responsabile del trattamento, in conformità all'articolo 32 del Regolamento UE 2016/679, hanno messo in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio. Le misure adottate garantiscono inoltre:

a) La pseudonimizzazione e la cifratura dei dati personali, ove possibile.

b) La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

c) La capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico.

d) Una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il Titolare del trattamento e il responsabile del trattamento assicurano che chiunque agisce sotto lo loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal Titolare del trattamento.

La sicurezza "*è l'insieme delle misure atte a garantire la disponibilità, l'integrità e la riservatezza delle informazioni gestite*".

Sono tre gli aspetti fondamentali relativi alla sicurezza delle informazioni:

- **Riservatezza**: solo gli utenti autorizzati possono accedere alle informazioni necessarie.
- **Integrità**: tutela dell'accuratezza e completezza dei dati.
- **Disponibilità**: le informazioni sono rese disponibili quando occorre e nell'ambito di un contesto pertinente.

Si riportano di seguito le misure di sicurezza adottate nell'ambito del trattamento dei dati effettuato da CPIA 2

9.1.1 Gestione operativa - misure di sicurezza fisica

Misure di sicurezza fisica	Note
Accesso agli uffici ove sono effettuati i trattamenti	L'accesso agli uffici è consentito previa identificazione dei visitatori all'ingresso dell'Istituto Comprensivo, eseguita da parte dei collaboratori scolastici incaricati. I visitatori sono successivamente accompagnati presso gli uffici
Sistemi di allarme/antintrusione	Gli uffici del CPIA 2 sono ospitati dagli Istituti Comprensivi. Il Titolare del trattamento, in questo caso, non ha un sistema di allarme di proprietà ma si avvale di quello dell'Istituto Comprensivo
Reception	Presente
Registrazione degli accessi all'Ufficio	Presente
Autenticazione degli accessi all'Ufficio	Presente sia per personale ata (badge fatti internamente) sia per docenti (firmano registro elettronico)
Chiusura delle porte locale server	Il server è presente presso l'ufficio del Dirigente Scolastico, non protetto in armadio rack. Oltre l'orario di lavoro ed in assensa del DS, le porte di accesso all'ufficio sono chiuse a chiave
Protezioni antisfondamento vetri	Non presenti

Custodia in classificatori o armadi chiusi a chiave	Presenti
Custodia dati in armadi blindati/ignifughi	Presenti
Dispositivi antincendio	Estintori
Porte tagliafuoco	Presenti
Gruppo di continuità	Non presenti
Schermatura cavi	Presente
Messa a terra	Presente
Climatizzazione sala server	Non presente
Presidio personale esterno	Non presente
Sala server situata in luogo non soggetto ad allagamenti	L'ufficio del Dirigente Scolastico è posizionato al 3° piano
Distruggi documenti	Presente
Aree di miglioramento: da acquistare gruppi di continuità	

9.1.2 Gestione operativa - misure di sicurezza logica

Misure di sicurezza logica	Note
Identificazione dell'Incaricato e/o Utente	Gli utenti accedono alla propria area di lavoro attraverso un account destinato alla funzione lavorativa, protetto da password
Autentificazione dell'Incaricato e/o Utente	Gli utenti accedono alla propria area di lavoro attraverso un account destinato alla funzione lavorativa, protetto da password
Profilazione utente	Non presente
Controllo degli accessi a dati e programmi	Non presente
Registrazione degli accessi	Non presente
Controlli aggiornati antivirus	Automatici
Sottoscrizione elettronica	Presente
Cifratura dei dati memorizzati	Presente
Cifratura dei dati trasmessi	Non presente
Annotazione della fonte dei dati	Non presente
Annotazione del Responsabile dell'operazione	Non presente
Monitoraggio continuo delle sessioni di lavoro	Non presente
Sospensione automatica delle sessioni di lavoro e riavvio con password	Presente
Verifiche periodiche sulle autorizzazioni dati e/o trattamenti consentiti	Non presente
Firewall	Presente
Inibizione accessi simultanei con medesimo account	Non presente
Sospensione automatica degli account	Non presente
Manutenzione sistemi e software	In base alle necessità
Sistemi di rilevazione disfunzioni	Firewall
Sistemi di rilevazione intrusione	Firewall
Aree di miglioramento: cambiare periodicamente le password	

9.1.3 Gestione operativa - misure di sicurezza organizzativa

Il datore di lavoro ha adottato misure organizzative e fisiche idonee a garantire che:

Misure di sicurezza organizzativa	Note
Analisi dei rischi	Nel presente documento
Classificazione dei dati	Nel presente documento
Linee guida per la sicurezza delle informazioni	Non presente
Linea guida su utilizzo degli strumenti scolastici	Non presente
Linee guida posta elettronica e internet	Non presente
Assegnazione di incarichi	Lettere di nomina persone autorizzate al trattamento
Mansionari e/o altre istruzioni interne	Non presente
Formazione	Da implementare
Back-up e disaster recovery	Il backup dei dati presenti sul server è eseguito giornalmente. Le copie dei backup sono salvate sia su 2 dischi esterni, collegati al server tramite porta USB, che su un server remoto di proprietà dell'Amministratore di Sistema. Tale server remoto è ubicato in Italia
Piano di manutenzione impianti	In conformità al d.lgs 81/08
Dichiarazione conformità impianti	In conformità al d.lgs 81/08
Procedure accessi	Non presente
Distruzione dei rifiuti elettrici ed elettronici in caso di smaltimento	Non si è ancora verificata la necessità di dover smaltire rifiuti elettrici ed elettronici
Assegnazione chiavi e codici	In possesso dei collaboratori scolastici
Politiche e procedure di sviluppo software	Non applicabile
Audit interni	Annuali in occasione degli audit del DPO
Controllo trattamenti effettuati da soggetti terzi	Lettere di nomina Responsabili esterni del trattamento
Aree di miglioramento: implementare piano di formazione in materia di protezione dei dati nei confronti delle persone autorizzate al trattamento; adottare linee guida per la sicurezza delle informazioni, su utilizzo degli strumenti scolastici, posta elettronica e internet; implementare procedura di smaltimento dei rifiuti elettrici e/o elettronici	

9.1.4 Gestione operativa - misure fisiche ed organizzative per il trattamento dei dati cartacei

Tutti gli armadi e i classificatori contenenti dati personali riservati sono ad accesso selezionato e muniti di serratura con chiavi custodite da personale individuato. Gli armadi e i classificatori della sede che risultassero non chiusi sono ubicati in uffici ad accesso selezionato. Si riporta la tabella delle responsabilità per la gestione degli archivi:

Archivio / armadio	Collocazione	Responsabile
Docenti e Personale ATA	Segreteria Archivio	Personale segreteria
Studenti	Segreteria Archivio	Personale segreteria

Il Regolamento interno per la sicurezza delle informazioni viene distribuito a tutti gli incaricati al fine di garantire che:

- i luoghi ove si svolge il trattamento di dati personali dei lavoratori sono opportunamente protetti da indebite intrusioni;
- le comunicazioni personali riferibili esclusivamente a singoli lavoratori avvengano con

modalità tali da escluderne l'indebita presa di conoscenza da parte di terzi o di soggetti non designati quali incaricati;

- siano impartite chiare istruzioni agli incaricati in ordine alla scrupolosa osservanza del segreto d'ufficio, anche con riguardo ai lavoratori del medesimo Titolare del trattamento che non abbiano titolo per venire a conoscenza di particolari informazioni personali;sia prevenuta l'acquisizione e riproduzione di dati personali trattati elettronicamente, in assenza di adeguati sistemi di autenticazione o autorizzazione e/o di documenti contenenti informazioni personali da parte di soggetti non autorizzati;
- sia prevenuta l'involontaria acquisizione di informazioni personali da parte di terzi o di altri lavoratori.

10 VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (P.I.A)

10.1 Fondamento giuridico

Il Regolamento UE 2016/679, all'articolo 35, richiede al Titolare del trattamento, allorché preveda di utilizzare nuove tecnologie per il trattamento dei dati personali, di effettuare, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali.

In particolar modo, la valutazione di impatto sulla protezione dei dati è richiesta nei seguenti casi:

- 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.
- Il trattamento su larga scala di categorie particolari di dati personali di cui all'articolo 9, o di dati relativi a condanne penali e a reati di cui all'articolo 10.
- La sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Considerata la tipologia dei dati trattati e le misure di sicurezza adottate dal CPIA 2, si è ritenuto opportuno non eseguire una Privacy Impact Assessment (P.I.A.) poiché i trattamenti eseguiti dal Titolare, considerati la natura, l'oggetto, in contesto e le finalità del trattamento, non possono comportare rischi elevati per i diritti e le libertà delle persone fisiche.

Pertanto, si ritiene opportuno procedere ad una analisi dei rischi generica all'interno di questo documento (vedi cap. 11).

11 ANALISI DEI RISCHI

Al fine di mettere in atto le misure necessarie a garantire la sicurezza dei dati e a tutelare i diritti e le libertà degli interessati, anche per rischi non legati specificatamente al trattamento dei dati personali, si è proceduto a individuare le categorie di rischi connessi alla gestione dei dati, valutando potenziali impatti in termini di Riservatezza (R), Disponibilità (D), Integrità (I).

Tipologia evento	Descrizione fonte di rischio	Impatto		
		R	D	I
Eventi Fisici	Incendio		X	X
	Allagamento		X	
	Manomissione		X	
	Terremoti		X	
	Fulmini e scariche atmosferiche		X	
Malfunzionamenti servizi	Guasto impianto di condizionamento		X	
	Sbalzi di tensione		X	
	Eccesso di traffico sulla rete		X	
	Disturbi elettromagnetici		X	X
Furto di informazioni e strumentazione	Intercettazioni (anche attraverso stampante)	X		
	Furto hardware	X	X	
	Furto dispositivi mobili	X	X	
	Furto di memorie o supporti esterni	X		
Anomalie IT	Malfunzionamento strumentazione IT		X	X
	Saturazione dei sistemi		X	X
	Malfunzionamenti applicativi scolastici	X	X	X
	Errori di manutenzione	X	X	X
	Virus e malware su pc	X	X	X
	Virus e malware su dispositivi mobili	X	X	X
	Non adeguata formattazione hw dismesso	X		
	Scadenza licenza software, interruzione degli aggiornamenti sulla sicurezza	X		X
Organizzazione /comportamento	Indisponibilità del personale		X	
	Cambio di personale	X	X	
	Rivelazione di informazioni a persone non autorizzate	X		
	Ricezione dati da origini non affidabili	X		
	Cancellazione erronea dei file		X	X
	Salvataggio file per uso personale	X		
Azioni non autorizzate	Uso non autorizzato dispositivi scolastici	X	X	X
	Uso di software non autorizzati	X	X	X
	Alterazione volontaria di informazioni	X	X	X
	Accesso non autorizzato alla rete	X		X
	Uso di strumentazione da parte di non autorizzate	X		X
	Accesso al DB da parte di non autorizzati	X		X
	Informazioni raccolte a seguito di non adeguata protezione all'insaputa dell'utente (es. senza screen saver)	X		
Uso non autorizzato di documenti cartacei	Fotocopie non autorizzate	X		
	Recupero di documenti scartati	X		
	Sottrazione di documenti cartacei	X		
	Riutilizzo di stampe contenenti dati personali	X		

Si riportano i criteri per definire il livello di impatto connesso agli eventi sopra descritti.
La probabilità di accadimento "P" è stabilita dall'analisi della storia recente dell'organizzazione, dalle segnalazioni dalle autorità di controllo e dalle linee guida e dai riferimenti bibliografici richiamati.

Livello	P – Probabilità di accadimento (almeno uno dei seguenti scenari)
1 Basso	- l'evento si può verificare con frequenza inferiore rispetto a quanto riportato dalle ricerche più note; - in caso di attacco deliberato, i dati sono poco appetibili e l'immagine aziendale non è compromessa e pertanto i tentativi di attacco o non sono iniziati o sono condotti da malintenzionati scarsamente preparati da un punto di vista tecnico e con scarse risorse a disposizione; - in caso di attacco non deliberato, l'ambito è poco complesso e quindi è difficile commettere errori; - in caso di eventi naturali, gli studi dimostrano che la minaccia può verificarsi molto raramente.
2 Medio	- la minaccia si può verificare secondo quanto riportato dalle ricerche più note; - in caso di attacco deliberato, i dati sono poco appetibili e l'immagine aziendale non è compromessa e quindi può essere condotto da malintenzionati non particolarmente motivati, mediamente preparati da un punto di vista tecnico e con scarse risorse a disposizione; o in alternativa, gli studi confermano che tentativi di attacco sono comunque rari; - in caso di attacco non deliberato, l'ambito è mediamente complesso e quindi possono essere commessi errori; - in caso di eventi naturali, gli studi dimostrano che la minaccia può verificarsi nella media dei casi studiati.
3 Alto	- la minaccia si può verificare più frequentemente rispetto a quanto riportato dalle ricerche più note; - in caso di attacco deliberato, i dati sono appetibili o l'immagine aziendale è compromessa, e quindi può essere condotto da malintenzionati molto motivati, tecnicamente preparati e con ingenti risorse a disposizione; o in alternativa, gli studi confermano che tentativi di attacco sono comunque portati molto di frequente; - in caso di attacco non deliberato, l'ambito è di elevata complessità (per esempio per molteplicità di sedi, tipologie di sistemi informatici, utenti interni e/o esterni) e quindi è facile siano commessi errori; - in caso di eventi naturali, gli studi dimostrano che la minaccia si verifica quasi certamente.

Si riportano i criteri per definire il livello di impatto connesso agli eventi sopra descritti.

D – Entità del danno			
Livello	**R- Riservatezza**	**I - Integrità**	**D- Disponibilità**
1 Basso	**Organizzazione** I dati non presentano particolari requisiti di riservatezza. I dati sono pubblici. **Interessati** La mancanza di riservatezza ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non presentano particolari requisiti di integrità. I dati gestiti non fanno parte di transazioni economiche, finanziarie o sanitarie. **Interessati** La mancanza di intergrità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente non comporta multe o penali rilevanti. **Interessati** La mancanza di disponibilità ha impatti lievi (p.e. fastidio) sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.
2 Medio	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti. **Interessati** La mancanza di disponibilità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.

D – Entità del danno			
Livello	**R- Riservatezza**	**I - Integrità**	**D- Disponibilità**
3 Alto	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine), ma un'eventuale loro diffusione non ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati non ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali non particolarmente rilevanti. **Interessati** La mancanza di disponibilità ha impatti, non critici (p.e. perdita di tempo, perdita limitata di serenità), sulla vita sociale o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.
4 Critico	**Organizzazione** I dati devono essere riservati per ragioni di business (concorrenza sleale, danni all'immagine) e un'eventuale loro diffusione ha elevati impatti sul business dell'organizzazione, sul rispetto della normativa vigente o sull'immagine dell'organizzazione. **Interessati** La mancanza di riservatezza ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** I dati non sono oggetto di transazioni di tipo economico, finanziario o sanitarie con impatti sul business di un'impresa. La mancanza di integrità dei dati ha elevati impatti sulle attività operative o sul rispetto della normativa vigente. **Interessati** La mancanza di integrità ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.	**Organizzazione** L'indisponibilità dei dati oltre i tempi stabiliti contrattualmente comporta multe o penali rilevanti. **Interessati** La mancanza di **disponibilità** ha elevato impatto sulla vita sociale (p.e. sconvolgendola) o personale degli interessati in termini di: - perdita di autonomia; - esclusione; - perdita di liberta; - danni fisici; - stigmatizzazione; - squilibrio di potere; - perdita di fiducia; - perdita economica.

Si riporta la stima della probabilità degli eventi sopra riportati, tenuto conto del potenziale impatto in termini di danno nei confronti dell'interessato e il conseguente livello di rischio associato.

Fattore di rischio	Probabilità	Impatto	Livello di rischio
Eventi fisici	1	2	2
Malfunzionamenti servizi	2	2	4
Furto di informazioni e strumentazione	2	2	4
Anomalie IT	2	2	4
Organizzazione /comportamento	2	2	4
Azioni non autorizzate	2	3	6
Uso non autorizzato di documenti cartacei	2	2	4

Valutazione dei livelli di rischio

P/D	Basso	Medio	Alto/Critico
Basso			
Medio			
Alto			

Livelli di rischio individuati e definizione dei controlli

1-2	Basso	Non necessitano interventi (buone prassi)
3-6	Medio	Azioni periodiche e programmate (Controllo operativo)
8-9	Alto	Azioni a breve termine
≥ 12	Critico	Azioni di immediata attuazione

12 DATA BREACH – Notifica della violazione dei dati all'autorità di controllo

Il Regolamento, all'art. 33 definisce che in caso di violazione dei dati personali, il Titolare o il Responsabile del trattamento procede senza indebiti ritardi e, ove possibile, non oltre 72 ore dopo esserne venuto a conoscenza, notifica la violazione dei dati personali all'autorità di controllo competente ai sensi dell'articolo 55, a meno che è improbabile che la violazione dei dati personali comporti un rischio per i diritti e le libertà delle persone fisiche. Se la notifica all'autorità di controllo non viene effettuata entro 72 ore, è accompagnata dai motivi del ritardo.

La notifica riporta i seguenti elementi:

a) descrizione della natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati e le categorie e il numero approssimativo di dati personali in questione;
b) nome e contatti del referente del Titolare o del Responsabile della protezione dei dati (DPO)
c) descrizione delle probabili conseguenze della violazione dei dati personali;
d) descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per
e) attenuarne i possibili effetti negativi.

Il Data Breach può riguardare essenzialmente:

- Riservatezza dei dati – divulgazione o accesso non autorizzato o accidentale di dati personali
- Disponibilità dei dati – alterazione non autorizzata o accidentale di dati personali
- Integrità dei dati – perdita accidentale o accesso non autorizzato di dati personali

La violazione può potenzialmente avere una serie di effetti negativi significativi sugli individui, che possono provocare danni fisici, materiali o immateriali, come ad esempio:

- perdita del controllo sui propri dati personali
- limitazione dei diritti
- discriminazione
- furto d'identità
- frode
- perdita finanziaria
- inversione non autorizzata di pseudonimizzazione
- danno alla reputazione
- perdita di riservatezza dei dati personali protetti dal segreto professionale.

Ogni possibile violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio sono riportate nel registro delle violazioni, compilato a cura del Titolare del Trattamento o del Responsabile della protezione dei dati.

13 TRASFERIMENTO DATI EXTRA UE

Il CPIA 2 non effettua il trasferimento dei dati in Paesi extra UE.
Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

14 GESTIONE DEI DIRITTI DELL'INTERESSATO

CPIA 2, in qualità di Titolare del trattamento, ha fornito a tutti gli interessati tutte le informazioni di cui agli articoli 13 e 14 del Regolamento Europeo 2016/679 e le comunicazioni di cui agli articoli 15 a 22 tramite le informative. L'interessato può esercitare il suo diritto contattando direttamente il titolare del trattamento all'indirizzo: mimm0cd00g@istruzione.it.

Al fine di garantire i diritti degli interessati, il Titolare del trattamento, supportato dal Responsabile del Trattamento o dal DPO, coinvolge le relative funzioni che possono fornire le risposte alle richieste degli interessati.

14.1 Diritto di accesso

Il Titolare del trattamento ha adottato misure idonee al fine di garantire agli interessati il diritto di ottenere la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di esercitare il "diritto di accesso" così come riconosciuto dall'articolo 15 del Regolamento UE 2016/679. L'interessato ha pertanto diritto di ottenere l'accesso ai dati personali che lo riguardano e alle seguenti informazioni:

a) Le finalità del trattamento.
b) Le categorie di dati personali in questione.
c) I destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali.

d) Quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo.

e) L'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento.

f) Il diritto di proporre reclamo a un'autorità di controllo.

g) Qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine.

h) L'esistenza di un processo decisionale automatizzato, compresa la profilazione di cui all'articolo 22, paragrafi 1 e 4 e almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

14.2 Diritto di rettifica

L'interessato, così come disposto dall'articolo 16 del Regolamento Europeo 2016/679, ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti e, tenuto conto delle finalità del trattamento, ha altresì il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

14.3 Diritto all'oblio

L'interessato, così come disposto dall'articolo 17 del Regolamento UE 2016/679, ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano qualora sussistano uno dei seguenti motivi:

a) I dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati.

b) L'interessato revoca il consenso su cui si basa il trattamento e se non sussiste altro fondamento giuridico per il trattamento.

c) L'interessato si oppone al trattamento e non sussiste alcun motivo legittimo prevalente per procedere al trattamento.

d) I dati personali sono stati trattati illecitamente.

e) I dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento.

f) I dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8.

14.4 Diritto di limitazione di trattamento

L'interessato, così come disposto dall'articolo 18 del Regolamento UE 2016/679, ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando:

a) L'interessato contesta l'esattezza dei dati personali, per il periodo necessario al titolare del trattamento per verificare l'esattezza di tali dati personali.

b) Il trattamento è illecito e l'interessato si oppone alla cancellazione dei dati personali e chiede invece che ne sia limitato l'utilizzo.

c) Benché il titolare del trattamento non ne abbia più bisogno ai fini del trattamento, i dati personali sono necessari all'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

d) L'interessato si è opposto al trattamento ai sensi dell'articolo 21 in attesa della verifica in merito all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.

14.5 Diritto alla portabilità dei dati

L'interessato, così come disposto dall'articolo 20 del Regolamento UE 2016/679, ha il diritto di ricevere i dati personali che lo riguardano forniti a un titolare del trattamento e ha altresì il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti.

14.6 Diritto di opposizione

L'interessato, così come disposto dall'articolo 21 del Regolamento UE 2016/679, ha il diritto di opporsi in qualsiasi momento al trattamento dei dati personali che lo riguardano.

L'interessato può esercitare il suo diritto contattando direttamente il Titolare del trattamento.

15 FORMAZIONE

15.1 Contesto generale

Tale capitolo del documento viene redatto al fine di definire le modalità di identificazione delle esigenze ed i criteri di attuazione del processo di addestramento del personale per il perseguimento delle strategie nel pieno rispetto della normativa vigente sul trattamento dei dati.

Scopo di questa attività è, inoltre, informare e formare costantemente il personale sui compiti assegnati, sulle responsabilità e sulle metodologie da applicare nell'esecuzione delle proprie attività, nell'ottica di un miglioramento continuo delle attività lavorative.

15.2 Gestione Operativa

Il personale verrà coinvolto in un processo di formazione/informazione in modo da assicurare la professionalità e le adeguate capacità degli incaricati per svolgere le attività di propria competenza.

In questo senso, l'attività formativa è rivolta a:

a) Fornire una preparazione professionale di base necessaria allo svolgimento dei compiti assegnati.
b) Permettere un continuo aggiornamento tecnico, reso necessario dall'evoluzione delle conoscenze tecniche ed informatiche.
c) Assicurare la corretta comprensione ed applicazione dei principi su cui si basa la Privacy Policy stabilita per il trattamento dei dati.

L'addestramento è previsto per:

d) Personale di nuova assunzione (comprensivo dell'affiancamento a persona esperta).
e) Personale assegnato a nuove mansioni.
f) Introduzione di nuove tecnologie informatiche.

l regolamento sull'uso dei sistemi informatici è consegnato ad ogni collaboratore, all'atto dell'avvio del rapporto di lavoro, insieme al regolamento interno.
Considerare procedure specifiche sulla dimissione del collaboratore, gestione lunga assenza e cambio mansione.

16 MONITORAGGIO PERIODICO

Periodicamente, con l'eventuale supporto dell'Amministratore di Sistema o altre aree scolastiche, il Titolare del Trattamento o DPO effettua delle verifiche sul corretto stato di applicazione delle procedure previste per il trattamento dei dati, verificando ad esempio le configurazioni di pc e dati trattati. Le verifiche sulla corretta applicazione dei principi relativi al trattamento dei dati si effettuano inoltre in occasione dell'aggiornamento annuale del presente documento.

A seguito di tali verifiche il Titolare del trattamento, in collaborazione con le funzioni coinvolte, stabilisce dei piani di miglioramento atti a prevenire il verificarsi di eventuali non conformità e a fornire una formazione continua al personale coinvolto nel trattamento dei dati.

17 PROGRAMMA DI MIGLIORAMENTO

In riferimento a quanto esposto nel capitolo 11 del presente documento, nella tabella sottostante viene riportato il programma individuato da CPIA 2 per il continuo miglioramento del sistema implementato:

Fattore di rischio	Probabilità	Impatto	Livello di rischio
Eventi fisici	1	2	2
Malfunzionamenti servizi	2	2	4
Furto di informazioni e strumentazione	2	2	4
Anomalie IT	2	2	4
Organizzazione /comportamento	2	2	4
Azioni non autorizzate	2	3	6
Uso non autorizzato di documenti cartacei	2	2	4

Fattore di Rischio	Descrizione intervento	Termine attuazione	Responsabile attuazione
Malfunzionamenti servizi	Acquistare i gruppi di continuità per i pc della segreteria	Prossimo audit del DPO	Titolare del trattamento Amministratore di Sistema
Furto di informazioni e strumentazione Azioni non autorizzate	Implementare procedura di smaltimento dei rifiuti elettrici e/o elettronici		
Uso non autorizzato di documenti cartacei	Si consiglia di monitorare periodicamente il corretto utilizzo dei dispositivi e degli archivi aziendali da parte del personale		
Organizzazione/ comportamento	Implementare piano di formazione in materia di protezione dei dati nei confronti delle persone autorizzate al trattamento		

18 ALLEGATI AL MODELLO ORGANIZZATIVO

Si riportano gli allegati al modello organizzativo per la gestione privacy del CPIA 2

LT	Informativa e consenso collaboratori P.IVA
LT	Informativa e consenso docenti e personale ATA
LT	Informativa e consenso alunni e famiglie
LT	Informativa candidati
LT	Informativa studenti
LT	Informativa bandi
LT	Privacy e cookies policy
LT	Nomina persone autorizzate al trattamento (docenti)
LT	Nomina persone autorizzate al trattamento (personale segreteria)
LT	Nomina Responsabile del trattamento con funzione di Amministratore di Sistema
LT	Nomina Responsabile esterno del trattamento
PO	Regolamento utilizzo strumenti informativi
PO	Procedura per l'esercizio dei diritti degli interessati
PO	Gestione Data Breach
RG	Registro violazioni
LT	Documenti Covid
LT	Informativa ad hoc servizio pago in rete
LT	Informativa alunni e famiglie + Pago in rete

Luogo Data

_____ _____

Titolare del trattamento dei dati

_____