Oxford Civezzano Società Cooperativa
gestore dell' ”Istituto Ivo de Carneri”

DPIA

Indice

Premessa

Il presente documento è redatto in continuità al DPS 2010 ed aggiornato secondo la normativa europea dall' avv. Mario Stefano Sforzellini del Foro di Trento sulla scorta dei dati esistenti e di altri forniti da personale amministrativo in alcuni incontri tenutesi presso la sede dell' Istituto Scolastico "Ivo de Carneri" delle singole scuole ed è emanato a cura del Titolare del Trattamento dei Dati in data 25 maggio 2018 in conformità a quanto disposto dall' art 35 GDPR, tenuto altresi conto degli articoli da 33 a 35 e dall'allegato B del Decreto Legislativo 30 giugno 2003 numero 196 e succ. mod..

Scopo del presente documento, di seguito denominato "DPIA", è quello di delineare il quadro delle misure di sicurezza, tecniche, informatiche, organizzative, logistiche e procedurali adottate e da adottare, da parte di questa società, relativamente al trattamento dei dati personali, nonchè, sulla scorta di quanto sopra, di apprezzare il grado di rischio e conseguentemente dei comportamenti da adottare al fine di mitigare eventuali impatti negativi sulla protezione dei dati raccolti per fini istituzionali.

Riferimenti normativi

Legge 07/08/1990 n. 241 e successive modifiche;

Legge 31/12/1996 n. 676, recante delega al governo in materia di tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

Legge 24/03/2001 n. 127, recante delega la governo per l'emanazione di un T. U. in materia di trattamento dei dati personali;

Decreto legislativo 30/06/2003 n. 196 – Codice in materia di protezione dei dati personali

- allegato B (Disciplinare tecnico in materia di misure minime di sicurezza);

Regolamento UE 27 aprile 2016 n. 679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

Obiettivi del documento

Il Documento consente al Titolare la valutazione preventiva di aspetti critici in ordine alla raccolta, trattamento e conservazione dei dati personali in possesso di Oxford Civezzano, soc.coop. gestore dell'Istituto Ivo de Carneri, al fine di mitigare eventuali aspetti di rischio con ulteriori procedure da individuare successivamente e comunque mira a implementare e garantire la riservatezza, la sicurezza e la protezione dei dati, nonché a porre in atto idonee strategie per la protezione delle aree e dei locali interessati a misure di sicurezza.

Il Documento garantisce che il trattamento dei dati si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il trattamento dei dati personali è disciplinato in modo da assicurare un elevato livello di tutela dei diritti e delle libertà degli interessati, nel rispetto dei principi di semplificazione, armonizzazione ed efficacia delle modalità previste per il loro esercizio da parte degli interessati, nonché per l'adempimento degli obblighi da parte del titolare del trattamento (art. 2 d.lgs. 196/2003).

Tali dati riguardano:

- il personale che presta servizio presso l'istituzione scolastica;
- gli alunni che frequentano questo Istituto;
- i genitori degli alunni o gli esercenti la potestà genitoriale per le notizie che trasmettono o portano a scuola;
- i fornitori.

In particolare, nel DPIA vengono definiti i criteri tecnici e organizzativi per:

1) la protezione delle aree e dei locali interessati dalle misure di sicurezza, nonché le procedure per controllare l'accesso delle persone autorizzate ad accedere ai medesimi locali;
2) i criteri e le procedure per assicurare l'integrità dei dati;
3) i criteri e le procedure per la sicurezza della trasmissione dei dati, cartacei o telematici;
4) l'elaborazione di un piano di formazione per rendere edotti gli incaricati del trattamento dei rischi che incombono sui dati e dei modi per prevenire gli eventi dannosi.

Dati generali

Soggetti che effettuano il trattamento

Titolare del trattamento

Il Titolare del trattamento è Oxford Civezzano S.C. gestore dell' "Istituto Ivo de Carneri" e la titolarità è esercitata dal legale rappresentante sig. Giovanni Scalfi.

Tra i compiti che normativamente sono assegnati al Titolare è prevista la vigilanza sul rispetto, da parte del Responsabile e degli Incaricati al trattamento dei dati, delle proprie istruzioni, nonché sulla puntuale osservanza delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza.

Il Titolare è il soggetto che assume le decisioni sulle modalità e le finalità del trattamento.

Responsabile del trattamento

Il Responsabile del trattamento è il soggetto preposto dal Titolare al trattamento dei dati personali. La designazione di un responsabile non esonera da responsabilità il Titolare il quale ha comunque l'obbligo di impartirgli precise istruzioni e di vigilare sull'attuazione di queste. Il Responsabile è un soggetto che fornisce, esperienza, capacità e affidabilità, idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza. Il Responsabile del trattamento dei dati personali, ai fini della sicurezza, ha le responsabilità indicate nella lettera di incarico.

Per il trattamento dei dati personali il Titolare ha nominato un Responsabile.

Incaricati del trattamento

Le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Titolare o del Responsabile. La designazione di ciascun Incaricato del trattamento dei dati deve essere effettuata, da parte del Titolare o del Responsabile, con lettera di incarico in cui sono ben specificati i compiti che gli sono affidati e l'ambito del trattamento consentito (art. 30 GDPR e art.30 comma 1 D. Legisl. 196/03).

Gli Incaricati del trattamento ricevono idonee ed analitiche istruzioni scritte, anche per gruppi

omogenei di lavoro, sulle mansioni loro affidate e sugli adempimenti cui sono tenuti. Agli incaricati deve essere assegnata una parola chiave ed un codice identificativo personale.

Nella tabella seguente sono elencati per gruppi gli incaricati del trattamento nominati mediante apposita lettera.

Incaricati	***Note***
Docenti	Incaricati, supplenti, assistenti educatori, collaboratori temporanei, preside e direttore
Personale amministrativo	Personale di segreteria e amministrazione interni all'istituzione
Personale ausiliario	Assistenti tecnici amministrativi esterni alla istituzione
Esterni	Assistenti educatori (eventuali)

Sede

Istituto Ivo de Carneri

Via Murialdo, 30

38045 Civezzano (TN)

Sedi periferiche

Nessuna

Elenco trattamenti *(Regola 19.1)*

Identificativo	***Descrizione sistetica***	***Categorie di interessati***	***Natura dei dati***		***Strumenti utilizzati***	***Altre strutture che concorrono al trattamento (anche esterne)***
			S	***G***		
001	Prenotazioni udienze	Alunni Insegnanti			Informatici Cartacei	
002	Gestione alunni Anagrafiche	Alunni	1,2, 5		Informatici Cartacei	Provincia Autonoma Trento
003	Gestione alunni certificati medici	Alunni	5		Cartacei	
004	Gestione alunni Diagnosi mediche di portatori di handicap	Alunni	5		Cartacei	
005	Registri di classe Registri insegnanti	Insegnanti Alunni	5		Cartacei	
006	Verbali scrutini Verbali esami	Insegnanti Alunni			Informatici Cartacei	
007	Archivio Registri insegnanti e classi, verbali scrutini ed esami	Insegnanti Alunni	5		Cartacei	
008	Gestione docenti Anagrafiche e servizio	Amministrativi Insegnanti	1,2, 3,5		Informatici Cartacei	Federazione Trentina Cooperative
009	Gestione docenti Certificati malattia	Amministrativi Insegnanti	5		Cartacei	Federazione Trentina Cooperative
010	Fascicolo personale	Amministrativi Insegnanti	1,2, 3,5		Cartacei	
012	Contabilità	Amministrativi Docenti Alunni Clienti Fornitori			Informatici Cartacei	Federazione Trentina Cooperative Commercialista Dott. Decarli Collegio sindacale
014	Gestione protocollo	Amministrativi Docenti Alunni Clienti Fornitori			Cartacei	
015	Gestione Patrimonio	Amministrativi			Informatici Cartacei	Federazione Trentina Cooperative Commercialista Dott.Decarli Collegio sindacale
016	Rendicontazione alla P.A.T. delle spese sostenute mediante contributo	Amministrativi Docenti Alunni Clienti Fornitori			Informatici Cartacei	Federazione Trentina Cooperative Commercialista Dott.Decarli Collegio sindacale Provincia di Trento (FSE, Servizio istruzione)
017	Trasferimento dati alunni ad altre scuole	Alunni	1,2, 5		Informatici Cartacei	Altre scuole
018	Iscrizioni alunni	Alunni	1,2, 5		Informatici Cartacei	

Identificativo	*Descrizione sistetica*	*Categorie di interessati*	*Natura dei dati*		*Strumenti utilizzati*	*Altre strutture che concorrono al trattamento (anche esterne)*
019	Trasferimento elenco alunni	Alunni	5		Informatici Cartacei	Comprensorio Servizio Istruzione PAT Ufficio FSE della PAT Servizio trasporti PAT Aziende (a fini assunzioni)
021	Dati presenze personale	Personale dell'Istituto	3,5		Informatici Cartacei	Federazione Trentina Cooperative
022	Dati statistici sugli alunni	Alunni			Informatici Cartacei	Servizio Istruzione PAT Ministero dell'istruzione
023	Dati sui portatori di Handicap	Amministrativi Docenti Alunni	5		Informatici Cartacei	Servizio Istruzione PAT
024	Richieste del personale	Amministrativi Docenti	4,5, 6		Cartacei	
028	Denunce Infortuni	Amministrativi Docenti Alunni	5		Informatici Cartacei	Servizio Istruzione PAT INAIL, Comune o Questura
030	Richieste visite mediche fiscali	Amministrativi Docenti	5		Cartacei	Medici fiscali INPS
031	Certificato Idoneità psicofisica	Alunni (iscritti a odontotecnico)	5		Cartacei	
032	Buoni Pasto	Alunni Alunni scuole medie Civezzano			Cartacei	Comprensorio Alta Valsugana
033	TELECAMERE Prevenzione di oggetti e cose da danni, furti e rapine. La registrazione permette di risalire all'autore di eventuali illeciti	Alunni Alunni scuole medie Civezzano Amministrativi Docenti			Registrazione su apposito apparato delle immagini riprese da 8 telecamere. Dati conservati per 5 giorni	

Legenda:

1. Dati personali idonei a rilevare l'origine razziale ed etnica
2. Dati personali idonei a rilevare le convinzioni religiose, filosofiche o di altro genere
3. Dati personali idonei a rilevare le opinioni politiche, l'adesione a partiti, sindacati
4. Dati personali idonei a rilevare l'appartenenza a partiti, sindacati, associazioni od organizzazioni carattere religioso, filosofico, politico o sindacale
5. Dati personali idonei a rilevare lo stato di salute e la vita sessuale

Dati aggiornati al 10 maggio 2018.

Distribuzione dei compiti e responsabilità *(Regola 19.2)*

Identificativo	***Struttura di riferimento***	***Referente***	***Incaricati***	***Trattamenti operati***
001	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe	Raccolta, consultazione, comunicazione, cancellazione
002	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe Docenti	Raccolta, Consultazione, Modificazione, Comunicazione, Diffusione, Cancellazione Archiviazione
003	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Comunicazione, Distruzione
004	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe Docenti	Raccolta, Consultazione, Comunicazione
005	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe Docenti	Raccolta, Consultazione, Modificazione, Comunicazione
006	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe Docenti	Raccolta, Consultazione, Modificazione, Comunicazione
007	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe Docenti	Raccolta, Consultazione, Comunicazione, Archiviazione
008	Amministrazione	Riccadonna Luca	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
009	Segreteria	Riccadonna Luca	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Comunicazione, Distruzione
010	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
012	Amministrazione	Riccadonna Luca	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione,

Identificativo	*Struttura di riferimento*	*Referente*	*Incaricati*	*Trattamenti operati*
				Comunicazione, Cancellazione Archiviazione
014	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
015	Amministrazione	Riccadonna Luca	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
016	Amministrazione	Riccadonna Luca	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
017	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
018	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
019	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
021	Amministrazione	Riccadonna Luca	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
022	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
023	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
024	Amministrazione	Riccadonna Luca	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
028	Amministrazione	Riccadonna Luca	Biondi Cristiana	Raccolta,

Identificativo	*Struttura di riferimento*	*Referente*	*Incaricati*	*Trattamenti operati*
			Riccadonna Ugo Lucente Giuseppe	Consultazione, Modificazione, Comunicazione, Cancellazione
030	Amministrazione	Riccadonna Luca	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
031	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Comunicazione
032	Segreteria	Biondi Cristiana Riccadonna Ugo Lucente Giuseppe	Biondi Cristiana Riccadonna Luca Riccadonna Ugo Lucente Giuseppe	Raccolta, Consultazione, Modificazione, Comunicazione, Cancellazione
033	Amministrazione	Riccadonna Luca	---	Raccolta, Consultazione, Cancellazione

Dati aggiornati al 10 maggio 2018.

Descrizione del sistema informativo

NOTA: l'istituto è dotato di aule informatiche, di PC portatili nei quali non vengono trattati dati personali. Tali aule e postazioni, utilizzate esclusivamente a fini didattici, pertanto sono state escluse dal presente documento.

Identificativo	***Sistema Operativo***	***Locale***	***Modello***	***CPU***	***MEM***	***HD***	***Host***
Host VMware	ESXi, 6.0.0	Locale server	HP ProLiant DL380p	Xeon E5-2620 6CPUs x 2 GHz	12GB	553,75 GB	
VM_Server2008 R2_61	Windows Server 2008 R2 Standard	VM		Xeon E5-2620 2CPUs x 2 GHz	4GB	180GB	Srv1
VM_srv02	Windows Server 2012 R2 Standard	VM		Xeon E5-2620 2CPUs x 2 GHz	6GB	60GB	SRV02
Server Backup	Windows Server 2008 R2 Standard	Ufficio Presidenza	HP	AMD Turion II Neo N54L	2GB	4TB	NAC23183
Segreteria	Windows 7 Pro SP1	Ufficio Segreteria	FUJITSU	i5-4460 3.2GHz	8GB	500GB	PC-UFF-01
Presidenza	Windows 7 Pro SP1	Ufficio Presidenza	Acer TravelMate	i3	4GB	250GB	??????
PC01	Windows 10 Pro	Ufficio Vice Preside	Intel NUC	i7-7567U 3.5GHz	8GB	1 TB	NUC
PC02	Windows 7 Pro SP1	Ufficio Segreteria	Dell	i3-4005 1.7GHz	4GB	250GB	AS-14-15-46
PC03	Windows 7 Pro SP1	Ufficio Segreteria	Samsung	i5-2510M 2.3GHz	4GB	128GB	PC

Identificativo	***Bios Pwd***	***User Pwd***	***Screen Saver Pwd***	***Backup***	***Personal Firewall***	***Antivirus***	***Correttivi***	***Rete***	***Dominio Gruppo di lavoro***
Host VMware	?	SI'(>8)		SI				192.168.1.60	
VM_Server2008R2_61	na	SI'(>8)	SI	SI		Nod32	Automatici	192.168.1.61	OXFORD
VM_srv02	na	SI'(>8)	SI	SI		Nod32	Automatici	192.168.100.1	
Server Backup	?	SI'(>8)	SI	na				192.168.1.75	
Segreteria	SI	SI'(>8)	SI	NO		Sophos	Automatici	192.168.1.11	OXFORD
Presidenza	SI	SI'(>8)	SI	NO		Sophos	Automatici	192.168.1.??	OXFORD
PC01	SI	SI'(>8)	SI	NO		Sophos	Automatici	192.168.1.20	OXFORD
PC02	SI	SI'(>8)	SI	NO		Sophos	Automatici	192.168.1.145	OXFORD
PC03	SI	SI'(>8)	SI	NO		Sophos	Automatici	192.168.1.31	OXFORD

RETI LOCALI ESISTENTI

Identificativo	***Rete***	***Locali***	***Postazioni***
OXFORD	192.168.1.0/24	Presidenza, Segreteria, Amministrazione, Corridoio	Tutte

Dati aggiornati al 10 maggio 2018

Misure di sicurezza

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

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

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

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

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

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

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

Attuale situazione relativa alle misure di sicurezza

Accesso fisico ai locali

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

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

Accesso fisico ai sistemi

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

Il server della scuola è posizionato all'interno di un armadio Rack chiuso, ubicato sul corridoio degli uffici amministrativi che hanno le porte chiuse a chiave doèp l' orario di lezione. Il corridoio è video sorvegliato in orario extrascolastico

Accesso logico ai sistemi

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

Antivirus

Tutte le postazioni della scuola, sono dotate di un sistema antivirus che viene tenuto aggiornato in automatico mediante o il server della rete locale (installazione centralizzata) o attraverso la connessione internet.

Backup

Il server della scuola è dotato di un sistema di backup dei dati che vengono salvati su un dispositivo dedicato posizionato in un locale con accesso riservato diverso da quello del server.

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

Vengono fatti dei salvataggi estemporanei dei dati del server su dischi USB esterni criptati e conservati al di fuori dell’edificio scolastico.

Disaster Recovery

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

Altre misure di sicurezza

Alimentazione elettrica

Il server è protetto da un sistema di continuità elettrica.

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

Accesso ad altre reti

La scuola accede ad Internet mediante collegamenti ADSL attraverso apparati UTM per firewalling,

content-filtering e gestione autenticazione utenti wi-fi.

Anti incendio

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

Applicazione correttivi ai sistemi

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

Trattamenti cartacei

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

Telecamere e videosorveglianza

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

Videocamere		Modalità
Quantità	Ubicazione	
2	I Piano	Visione e registrazione fuori orario didattico
3	II Piano	Visione e registrazione fuori orario didattico
3	III Piano	Visione e registrazione fuori orario didattico

Analisi del rischio *(art 35 GDPR - Regola 19.3)*

Evento			*Descrizione e impatto sulla sicurezza*
Comportamenti degli operatori	E001	Sottrazione di credenziali di autenticazione	**Descrizione:** Le credenziali (es. Nome Utente/parola chiave) possono essere sottratte al legittimo possessore con vari metodi o scoperte anche grazie alla negligenza nella conservazione da parte del possessore stesso.
			Impatto: Altri soggetti possono accedere alle banche dati protette con tali credenziali sostituendosi in tutto e per tutto al soggetto possessore delle stesse. Il sistema di protezione non può in principio sapere dell'occorrenza di tale furto.
	E002	Carenza di consapevolezza, disattenzione o incuria	**Descrizione:** A causa di impreparazione, anche tecnica, degli strumenti utilizzati e delle procedure messe a disposizione, gli incaricati del trattamento possono compiere operazioni errate.
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati.
	E003	Comportamenti sleali o fraudolenti	**Descrizione:** Con comportamento consapevole, derivante potenzialmente da vari fattori quali (risentimenti verso la scuola, il perseguimento di fini personali, etc.) gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati interessata l'evento.
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.
	E004	Errore materiale	**Descrizione:** A causa di negligenza, scarsa conoscenza degli strumenti a disposizione o distrazione, gli incaricati del trattamento possono compiere operazioni errate o specificare dati errati.
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati.
	E005	Comportamenti illegali a seguito di minacce	**Descrizione:** In conseguenza di pressioni di vario tipo (es. minacce, ricatti, pressioni psicologiche, ecc...) gli incaricati del trattamento possono compiere operazioni illecite sulla banca dati interessata l'evento.
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.
Eventi relativi agli	E101	Azione di virus informatici o di programmi suscettibili di recare danno	**Descrizione:** Sul sistema su cui si trova la banca dati interessata all'evento o il software utilizzato per accedervi, può introdursi un virus informatico o altro programma dannoso
			Impatto: Nei casi più gravi si può arrivare alla distruzione dell'intera banca dati. Nei casi meno gravi si può avere un malfunzionamento del sistema. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.

Evento			*Descrizione e impatto sulla sicurezza*
strumenti	E102	Spamming o tecniche di sabotaggio	**Descrizione:** Il sistema di posta utilizzato dagli incaricati del trattamento potrebbe essere obiettivo di invii di posta non richiesta e fasulla generata anche con strumenti automatizzati. Tali messaggi possono contenere false notizie.
			Impatto: Gli incaricati del trattamento possono erroneamente prendere in considerazione tali notizie ed operare interventi sulle banche dati non corretti.
	E103	Malfunzionamento, indisponibilità degli strumenti	**Descrizione:** I sistemi HW/SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono avere malfunzionamenti da cui possono derivare impossibilità di azioni reali sui dati o creare inconsistenza nelle banche dati.
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati.
	E104	Degrado degli strumenti	**Descrizione:** I sistemi HW/SW con i quali vengono manipolati i dati oggetto dell'evento da parte degli incaricati, possono essere soggetti a degrado naturale conseguente all'uso o al solo funzionamento. Da ciò possono derivare impossibilità di azioni reali sui dati o creare inconsistenza nelle banche dati.
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati.
	E105	Accessi esterni non autorizzati	**Descrizione:** Soggetti in possesso di credenziali di accesso al sistema, o intenzionati a sferrare un attacco informatico ad uno dei sistemi HW/SW da cui è possibile intervenite su una banca dati obiettivo, possono accedere al sistema individuato da una postazione non utilizzata in condizioni normali di operatività per accedere a tale sistema.
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottenere un contenuto errato nella banca dati. In certi casi l evento può comportare la sottrazione, in modo illecito, di dati.
	E106	Intercettazione di informazioni in rete	**Descrizione:** Soggetti malintenzionati possono catturare, mediante vari sistemi fisici, parte delle informazioni che transitano sulla rete informatica della scuola o sulla rete di collegamento con altri Enti. Ciò può avvenire in un qualunque punto tra il sistema utilizzato e il sistema HW/SW degli incaricati.
			Impatto: Nei casi più gravi, mediante varie tecniche, si può giungere alla distruzione o manipolazione dei dati. In generale si può avere una sottrazione di dati da parte dei malintenzionati.
Eventi relativi al co	E201	Accessi non autorizzati a locali da cui è possibile accedere ai dati	**Descrizione:** Un soggetto autorizzato o non allo scopo, può comunque accedere fisicamente ai locali presso i quali è accessibile e manipolabile la banca dati interessata all'evento.
			Impatto: Nei casi più gravi si può ottenere la distruzione di tutta o parte della banca dati. Nei casi meno gravi si ottiene un contenuto errato nella banca dati. In certi casi l'evento può comportare la sottrazione, in modo illecito, di dati.

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

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

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

Misure da adottare (art 35 GDPR - Regola 19.4)

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

- aggiornamento periodico (minimo una volta l'anno) dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici con relativa segnalazione al titolare o al responsabile del trattamento
- mantenimento delle misure di prevenzione per eliminare gli eventuali incendi con adeguate modalità di gestione degli stessi (impianto elettrico a norma, idranti, estintori, disponibilità degli spazi per l'ingresso dei mezzi dei Vigili del Fuoco, etc.);
- regolamentazione nell'accesso ai locali e alle attrezzature che conservano dati, archivi e documentazione;
- i locali contenenti dati personali sensibili o giudiziari devono rimanere chiusi a chiave quando nessun incaricato è all'interno;
- valutazione di attuazione di misure di protezione attiva e passiva dei locali ove si trattano dati personali (sistemi allarme, porte di ferro, inferriate, protezione di accesso agli uffici di direzione, segreteria, archivio, sala insegnanti);
- controllo periodico del buon esito del salvataggio dei dati del server su unità rimovibili;
- istruzioni a tutti gli incaricati affinché non rimangano dati personali abbandonati sui singoli posti di lavoro;
- adozione di procedure per la custodia di copie di sicurezza e per il ripristino della disponibilità dei dati e dei sistemi in caso di distruzione o danneggiamento;
- periodica (almeno ogni tre mesi) verifica della funzionalità e dell'efficienza delle misure di protezione e delle strutture operative responsabili, anche mediante la compilazione di apposite schede di monitoraggio;
- adozione di procedure di gestione delle credenziali di autenticazione;

1. CRITERI, PROCEDURE PER GARANTIRE L'INTEGRITA' DEI DATI

Il Titolare o il Responsabile del trattamento con il supporto di un esperto informatico (alla redazione del presente documento il sig. Giorgio Bertoldini), stabilisce la periodicità con cui debbono essere effettuate le copie di sicurezza delle banche dei dati trattati. In particolare per ogni banca dati devono essere definite le seguenti specifiche:

- il tipo di supporto da utilizzare per le copie di back-up;
- il numero di copie di back-up effettuate ogni volta;
- se i supporti utilizzati per le copie di back-up sono riutilizzati e in questo caso con quale periodicità;
- se per effettuare le copie di back-up si utilizzano procedure automatizzate e programmate;
- trasposizione dei dati informatici su unità rimovibili;
- la durata massima stimata di conservazione delle informazioni senza che ci siano perdite o cancellazione di dati;
- gli Incaricati del trattamento ai quali è stato assegnato il compito di effettuare le copie di back-up.

2. CUSTODIA E CONSERVAZIONE DELLE COPIE DI BACK-UP

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

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

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

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

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

3. PROTEZIONE DA VIRUS INFORMATICI

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

sistemi disponibili sul mercato.

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

E' opportuno che gli Incaricati che utilizzano i sistemi informatici annotino gli eventuali virus rilevati, e, se possibile, la fonte da cui sono pervenuti, al fine di isolare o comunque trattare con precauzione i possibili portatori di infezioni informatiche.

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

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

4. PROTEZIONE DELLE AREE E DEI LOCALI

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

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

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

Criteri e procedure per il ripristino della disponibilità dei dati

(art 35 GDPR - Regola 19.5)

Banca dati / data base / archivio dati	***Criteri e procedure per il salvataggio e il ripristino dei dati***	***Pianificazione delle prove di ripristino***
Dati presenti sul server	Salvataggio giornaliero su supporto esterno	Almeno 2 volte l'anno il Titolare o il Responsabile provvede a far eseguire da un tecnico informatico delle prove di ripristino dei dati
Dati presenti sulle postazioni di lavoro	Salvataggio ad ogni utilizzo su supporto esterno o mediante chiavette USB	Almeno 2 volte l'anno il Titolare o il Responsabile provvede a far trasferire sul server i dati eventualmente presenti sulle postazioni di lavoro

Formazione degli incaricati (art 35 GDPR - Regola 19.6)

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

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

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

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

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

Interventi formativi programmati

Data	***Titolo***	***Descrizione***	***Numero di incaricati***
---	---	---	---

Pianificazione degli interventi formativi previsti

Descrizione sintetica degli interventi formativi	***Classi di incarico o tipologie di incaricati interessati***	***Tempi previsti***
Nozioni di base di sicurezza informatica. Presentazione del GDPR e approfondimento dei concetti di informativa, consenso, figure coinvolte. Presentazione delle misure minime di sicurezza e loro implementazione in una realtà scolastica.	Personale amministrativo Docenti e ATA	Entro ottobre 2018

Trattamenti affidati all'esterno (art 35 GDPR - Regola 19.7)

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

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

Descrizione sintetica dell'attività "esternalizzata"	***Trattamenti di dati interessati***	***Soggetto esterno***	***Descrizione dei criteri e degli impegni assunti per l'adozione delle misure***
Gestione docenti anagrafiche e servizio	Dati personali	Federazione Trentina Cooperative in qualità di titolare autonomo di trattamento	Il soggetto esterno dovrà dichiarare di ottemperare agli obblighi previsti dal GDPR per la protezione dei dati personali; dovrà inoltre relazionare annualmente sulle misure di sicurezza adottate ed allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.
Gestione personale Certificati di malattia Dati presenze personale	Dati personali anche sensibili	Federazione Trentina Cooperative in qualità di titolare autonomo di trattamento	Il soggetto esterno dovrà dichiarare di ottemperare agli obblighi previsti dal GDPR per la protezione dei dati personali; dovrà inoltre relazionare annualmente sulle misure di sicurezza adottate ed allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.
Contabilità Gestione Patrimonio Rendicontazione alla PAT delle spese sostenute mediante contributo	Dati personali	- Federazione Trentina Cooperative - Studio Decarli - Revisore Contabile PAT in qualità di titolari autonomi di trattamento	Il soggetto esterno dovrà dichiarare di ottemperare agli obblighi previsti dal GDPR per la protezione dei dati personali; dovrà inoltre relazionare annualmente sulle misure di sicurezza adottate ed allertare immediatamente il proprio committente in caso di situazioni anomale o di emergenze.

Certificazioni rilasciate dagli esterni (artt 42 e ss. GDPR).

Al momento non sono presenti certificazioni di esterni.

Conclusioni

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

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

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

Civezzano, 24 maggio 2018 Il Titolare del Trattamento

Il legale rappresentante Giovanni Scalfi

OXFORD CIVEZZANO
Societa' Cooperativa
Via Murialdo, 30
38045 CIVEZZANO (TN)
P. IVA e C.F.: 01572180220