LICEO SCIENTIFICO STATALE "F.REDI" "F. REDI"

VIA LEONE LEONI, 38, 52100, AREZZO, AR

Tel. 0575/27633, Email: segreteria@liceorediarezzo.it

Prot. n. 2835 /G1 Arezzo, 31/03/2017

Il Dirigente Scolastico, Prof. Anselmo Grotti, in qualità di legale rappresentante pro tempore dell' istituzione scolastica indicata in intestazione (in prosieguo denominata istituto),

- Visto il decreto legislativo 30 giugbo 2003 n. 196 recante il Codice in materia di protezione di dati personali, e segnatamente gli artt. 33 e ss., nonchè l'allegato B del suddetto decreto, contenente il Disciplinare tecnico in materia di misure minime di sicurezza;
- Considerato che l'istituto scolastico è titolare del trattamento di dati personali ai sensi dell'art. 28 del D.Lgs. n.196 del 2003;
- Visto l'obbligo di prevedere ed applicare le misure minime di sicurezzad i cui agli artt. 31 e ss. del D.Lgs. n.196 del 2003;
- Visto il Regolamento recante identificazione dei dati sensibili e giudiziari trattati e delle relative operazioni effettuate dal Ministero della Pubblica Istruzione, emanato con Decreto Ministeriale n.305 del 7.12.2006;
- Atteso che la suddetta istituzione scolastica è tenuta a prevedere ed applicare le misure minimem di sicurezza di cui agli arrt. 31 e ss. del D.Lgs. n.196 del 2003, adotta il presente

DOCUMENTO PROGRAMMATICO DELLA SICUREZZA

1. Finalità

Il presente documento, elaborato al fine di mettere in atto le misure di sicurezza per tutelare i dati personali oggetto di trattamento, contiene idonee informazioni riguardanti:

- i trattamenti dei dati personali effettuati dal personale dell'istituto scolastico;
- la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;
- l'analisi dei rischi che incombono sui dati;
- le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonchè la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;
- la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento degli stessi o degli strumenti informatici;
- gli interventi formativi degli incaricati predisposti al trattamento dati, al fine di renderli edotti sui rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare;
- i criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati all'esterno della struttura del titolare.

Il presente documento è sottoposto a revisione annuale entro e non oltre la scadenza del 31 marzo, e comunque tempestivamente aggiornato in caso di inadeguatezza delle misure di sicurezza adottate o variazioni relative a uno qualsiasi dei contenuti del documento medesimo di cui ai punti sopra riportati (individuati).

Gli allegati al presente documento formano parte integrante dello stesso.

Per le attività correlate alla gestione del sistema di protezione dei dati personali trattati presso o per conto

dell'istituto, il personale incaricato si avvale del software Argo Privacy Web, applicativo Web prodotto e manutenuto dalla Argo Software s.r.l., e per il quale l'istituto ha provveduto a formalizzare l'incarico in qualità di Responsabile esterno del trattamento, con adeguata lettera di nomina.

2. Elenco dei trattamenti

Nel perseguimento delle finalità istituzionali, l'istituto scolastico è Titolare del trattamento di dati (sia comuni che sensibili e giudiziari) relativi a studenti, personale dipendente e fornitori. La descrizione dettagliata dei trattamenti effettuati è riportata sull'allegato titolato "Elenco dei trattamenti". In considerazione del fatto che alcuni dei trattamenti effettuati dall'istituto vengono svolti con l'ausilio di strumenti elettronici, si è provveduto a corredare il presente documento con le informazioni relative agli elaboratori utilizzati, riportati sull'allegato "Elenco hardware".

3. Responsabilità

Il seguente funzionigramma dell'istituto fornisce una descrizione della struttura dell'organizzazione scolastica e degli ambiti di competenze delle singole unità operative e delle figure preposte al trattamento dei dati.

Figure - Unità operative	Funzioni
Dirigente scolastico	In qualità di rappresentante legale dell'istituzione, è il responsabile della gestione del sistema di tutela e protezione dei dati trattati presso o per conto dell'istituto scolastico. In qualità del ruolo ricoperto all'interno dell'organizzaione: • designa, con atto di nomina individuale, gli incaricati e le altre figure del sistema di gestione privacy; • vigila sul loro operato, verificando, la puntuale osservanza delle istruzioni impartite, in base alle funzioni attribuite; • redige il presente documento, coaudivato dai responsabili del trattamento.
Responsabili del trattamento	È individuato dal dirigente scolastico tra i soggetti che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, in specie sotto il profilo della sicurezza. È designato con atto di nomina individuale, recante descrizione analitica delle funzioni attribuite, concernenti: • l'organizzazione delle operazioni di trattamento dei dati; • l'individuazione e aggiornamento degli incarichi e dei loro ambiti di trattamento; • la vigilanza del rispetto delle istruzioni impartite agli incaricati del trattamento; • la conservazione e custodia dei supporti utilizzati per le copie dei dati; • la conservazione e custodia della documentazione concernente il sistema di gestione privacy (DPSS e suoi allegati, lettere di nomina, verbali ecc.); • il monitoraggio delle misure di sicurezza adottate. Per ragioni organizzative, il dirigente scolastico può nominare più responsabili del trattamento con ambiti di operatività distinti. La nomina di responsabile può riguardare anche soggetti esterni all'istituto scolastico, operanti in nome e per conti dello stesso.

Amministratori di sistema	In base al provvedimento del Garante del 27/11/2008, recante descrizione delle misure e degli accorgimenti prescritti ai titolati dei trattamenti effettuati con strumenti informatici relativamente all'attribuzione delle funzioni di amministratore di sistema, con questa figura vengono individuati quanti all'interno dell'istituto svolgono funzioni relative alla gestione e alla manutenzione di impianti di elaborazione con cui vengono effettuati trattamenti di dati personali, compresi i sistemi di gestione delle base dati, le reti locali e gli apparati di sicurezza, nella misura in cui consentono di intervenire sui dati personali. È designato dal dirigente scolastico con atto di nomina individuale tra i soggetti che per esperienza, capacità e affidabilità forniscono idonea garanzia del pieno rispetto delle disposizioni vigenti in materia di trattamento, in particolar modo sotto il profilo della sicurezza. Sulla lettera di nomina sono descritti analiticamente gli ambiti di operatività consentiti. In qualità del suo ruolo: • coadiuva il responsabile del trattamento nel definire le misure e gli accorgimenti utili ad una efficace gestione delle copie di sicurezza degli archivi elettronici; • presiede alla funzione di attribuzione delle credenziali e dei privilegi degli utenti del sistema informatico; • sovrintende al funzionamento della rete, di backup e di disaster recovery dei dati; • predispone idonei strumenti di registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici effettuati in qualità di amministratore di sistema; • predispone sistemi idonei a garantire la completezza, inalterabilità e integrita delle predette registrazioni. L'operato dell'amministratore è oggetto con cadenza almeno annuale ad un'attività di verifica da parte della direzione scolastica, al fine di controllare la sua rispondenza alle misure organizzative, tecniche e di sicurezza previste dalle norme vigenti.
Responsabili controllo accessi ai locali	A questa figura è demandato il compito di sovrintendere ai sistemi di gestione e controllo degli accessi ai locali che gli sono stati affidati
Preposti alla custodia delle password	È incaricato della conservazione e custodia delle copie di credenziali di accesso, utilizzate dagli operatori addetti all'utilizzo degli strumenti informatici.

Incaricati del trattamento	In base alla definizione riportata all'art. 30 del Codice in materia di protezione dei dati personali, nell'ambito dei trattamenti svolti all'interno dell'istituto scolastico, devono intendersi incaricati del trattamento: • il personale docente (per il trattamento dei dati relativi agli alunni); • il personale amministrativo (per il trattamento dei dati connesso alla gestione amministrativa di alunni, personale scolastico e fornitori); • il personale ausiliario (per il trattamento dei dati derivanti dalla fotocopiatura di documenti, trasmissione di comunicazioni, ricezione e invio di fax); • eventuale personale esterno coinvolto nella realizzazione delle attività progettuali previste dal POF d'istituto, nella misura in cui svolgano operazioni di trattamento di dati personali relativi ad alunni o ad altro personale scolastico.
Gruppo Privacy	La commissione, istituita dalla direzione scolastica al fine di coadiuvare la stessa nella gestione delle questioni attinenti la privacy è composta da personale interno con comprovate conoscenze giuridiche e/o tecnologiche e si occupa di segnalare ai rapprensentanti della direzione o ai responsabili del trattamento, eventuali innovazioni di natura normativa o tecnologica che possono rendere inadeguato il sistema di gestione privacy dell'istituto e di proporre nuove misure e accorgimenti per la protezione dei dati.

L'elenco dei responsabili del trattamento, degli amministratori di sistema e delle altre figure del sistema di gestione privacy (ad eccezione degli incaricati non addetti all'utilizzo di strumenti informatici) e delle funzioni ad essi attribuite, è riportato sull'allegato titolato "Mansionario".

Il Mansionario è affisso all'albo e pubblicato nell'intranet istituzionale per darne massima conoscenza a tutto il personale.

All'atto della nomina vengono consegnate all'incaricato le linee guida, recanti istruzioni operative relative all'ambito di trattamento consentito, in funzione del profilo professionale di appartenenza.

Agli addetti alla segreteria amministrativa didattica e del personale è delegata la funzione di fornire le informative agli interessati e/o dare adeguate informazioni per la consultazione delle stesse sul sito istituzionale.

4. Analisi dei rischi e programma delle misure di prevenzione e protezione

Mutuando il modello del miglioramento continuo dei sistemi di qualità (Plan – Do – Check - Act), il sistema di protezione dei dati personali (in prosieguo denominato sistema di gestione privacy) si compone di 4 fasi:

- analisi dei rischi e pianificazione degli interventi di adeguamento;
- attuazione delle misure di sicurezza idonee;
- monitoraggio dell'efficacia del sistema di gestione privacy;
- attuazione delle misure correttive

4.1. Analisi dei rischio e pianificazione degli interventi di adeguamento

Il processo di analisi dei rischi ha inizio con una ricognizione:

- delle banche dati presenti;
- dei trattamenti effettuati;
- delle misure di sicurezza presenti (v. "Elenco delle misure adottate");
- delle criticità emerse nel periodo intercorso dall'ultima revisione del documento programmatico sulla sicurezza, raccolte attraverso le schede di segnalazione e opportunamente registrate sul sistema Argo Privacy Web.

Per l'attività di analisi vengono prese in considerazione gli eventuali rischi relativi a:

- protezione dei locali
- protezione integrità dei dati automatizzati
- protezione dei dati trattati con strumenti non automatizzati
- protezione della trasmissione dati

Per la valutazione dei rischi, viene messa in correlazione la probabilità di accadimento di un evento dannoso (P) con la "magnitudo" del danno che potrebbe conseguirne (D).
La stima del livello di rischio è espressa come prodotto dei due indici: R = PxD
La probabilità e la magnitudo, misurate in scala 1-4, danno origine alla seguente matrice di rischio

	MAGNITUDO			
PROBABILITÀ	**1 (nessun danno)**	**2 (danni lievi)**	**3 (danni medi)**	**4 (danni gravi)**
4 (alta)	4	8	12	16
3 (media)	3	6	9	12
2 (bassa)	2	4	6	8
1 (nulla)	1	2	3	4

Il rischio è valutato sulla base della seguente legenda

	rischio accettabile
	rischio basso
	rischio medio
	rischio elevato

È chiaro che più alto è il rischio, maggiore deve essere l'urgenza con cui intervenire.

L'output del processo di analisi e di valutazione dei rischi è costituito dall'allegato titolato "Analisi dei rischi".
La pianificazione degli interventi migliorativi tiene conto dell'ordine di priorità emerso dall'analisi dei rischi. Gli interventi definiti in questa fase sono descritti sull'allegato titolato "Piano di miglioramento", sul quale vengono altresì riportati - per ciascun intervento - il termine temporale entro il quale procedere al completamento dell'azione e il responsabile della sua esecuzione.

4.2. Attuazione delle misure di sicurezza idonee

Il responsabile del trattamento delegato vigila sull'attuazione delle misure di sicurezza e periodicamente aggiorna lo stato di esecuzione degli interventi pianificati, registrando per ciascuna azione, sul sistema Argo Privacy Web, l'esito delle verifiche.

Il dirigente scolastico prende visione attraverso il suddetto sistema, dello stato complessivo di attuazione del piano di miglioramento e, sulla base delle evidenze, pianifica eventuali ulteriori azioni.
Per quanto attiene, l'installazione di dispositivi di sicurezza per la protezione dei dati personali da parte di soggetti esterni, secondo quanto disposto dal punto 25 del disciplinare tecnico, allegato B al Codice di protezione dei dati personali, l'installatore rilascia alla segreteria amministrativa dell'istituto unadichiarazione di conformità dei dispositivi installati, debitamente compilata e firmata.

4.3. Monitoraggio dell'efficacia del sistema di gestione privacy

La direzione, consapevole dell'importanza fondamentale rivestita da questo processo all'interno del sistema di gestione privacy, ritiene che l'implementazione di un'efficace sistema di controllo richieda necessariamente il coinvolgimento di tutto il personale della scuola.

In questo senso, si è ritenuto opportuno garantire il monitoraggio attraverso la raccolta delle segnalazioni pervenenti dal personale coinvolto nelle operazioni di trattamento e dagli addetti al sistema di gestione privacy dell'istituto: le segnalazioni raccolte mediante i moduli disponibili negli uffici di segreteria del personale e nell'intranet istituzionale (v. "Scheda di segnalazione"), vengono caricate ad opera del responsabile del trattamento, sul sistema Argo Privacy Web. L'allegato "Report Segnalazioni", elaborato dal sistema Argo Privacy Web, fornisce il report delle segnalazioni pervenute ed è sottoposto all'analisi della direzione per l'adozione delle opportune azioni correttive.

4.4. Ripristino della disponibilità dei dati informatizzati

Per rispondere in maniera efficiente a situazioni di emergenza quali la distruzione o il danneggiamento dei dati o degli strumenti elettronici con cui avviene il trattamento degli stessi, per ogni banca dati informatica, la direzione scolastica ha provveduto ad individuare tra gli operatori degli applicativi informatici di gestione delle suddette banche dati, i preposti all'esecuzione delle copie di sicurezza degli stessi (backup operator). Le modalità e i preposti all'esecuzione dei backup sono indicati sull'allegato "Scheda Backup".
Le prove di ripristino sono eseguite dagli stessi con cadenza settimanale. In caso di esito negativo della prova di ripristino, l'operatore segnala repentinamente l'anomalia al responsabile del trattamento, per la messa in atto delle azioni opportune per il recupero dei dati (es. invio delle copie di backup alla ditta che effettua la manutenzione degli archivi, richiesta di copie esternalizzate).
Eventuali documenti di office automation contenenti dati personali, vengono masterizzati dagli autori degli stessi su c-rw/dvd con frequenza settimanale e i supporti consegnati al responsabile del trattamento per la loro conservazione.

4.5. Utilizzo della posta elettronica e di Internet

La direzione scolastica, considerata la necessità di contemperare l'obbligo di adozione di misure di protezione dei dati trattati con strumenti informatici e di prevenzione dei rischi che incombono sugli stessi a seguito dell'utilizzo della posta elettronica e di internet, con l'esigenza di tutelare la dignità dei lavoratori e il diritto alla riservatezza dei loro dati personali, ha adottato un disciplinare interno, al fine di descrivere le caratteristiche e le regole di utilizzo della rete Internet e della posta elettronica ,e di informare i lavoratori sui controlli effettuati e sul trattamento eseguito sui loro dati personali in conseguenza delle misure adottate per la protezione degli strumenti informatici.
Il disciplinare è aggiornato con cadenza almeno annuale, in occasione della revisione periodica del presente documento, o in caso di rinvenimento di soluzioni tecnologiche ritenute più idonee a tutelare i dati personali dei lavoratori, e portato a conoscenza di tutti i lavoratori mediante affissione all'albo dell'istituto e pubblicazione nell'intranet istituzionale.

5. Formazione degli incaricati
Conformemente a quanto disposto dal punto 19.6 del Disciplinare tecnico in materia di misure minime di sicurezza, interventi formativi del personale sono programmati già al momento dell'ingresso in servizio degli incaricati, nonchè in occasione di cambiamenti di mansioni o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali.
È compito del responsabile del trattamento delegato:

- rilevare il bisogno di interventi formativi;
- organizzare gli stessi compatibilmente con le esigenze dell'attività lavorativa;
- redigere il piano di formazione;
- raccogliere l'elenco dei partecipanti di ogni singolo corso e informarli dettagliatamente sullo stesso (contenuti, obiettivi, modalità di svolgimento, ecc.);
- vigilare sul rispetto del programma dell'attività formativa;
- vigilare sulla partecipazione dei corsisti.

Il dirigente scolastico può autorizzare la partecipazione del personale a corsi organizzati e tenuti esternamente alla sede dell'istituto. In tal caso le attività di controllo dell'attività formativa e della partecipazione dei corsisti saranno a carico dall'Ente che organizza il corso , il quale provvederà a darne comunicazione al dirigente scolastico.

6. Trattamenti affidati in outsourcing
In caso di sussistenza dell'esigenza di affidare trattamenti di dati a terzi, l'istituto si avvale unicamente di soggetti con compravata esperienza e affidabilità in materia di protezione dei dati personali. Da ogni soggetto esterno, l'istituto riceve descrizione delle modalità di trattamento e delle misure di sicurezza adottate per garantire la protezione dei dati stessi. I documenti contenenti le descrizioni di cui sopra, sono conservate a cura del responsabile del trattamento insieme alla restante documentazione del sistema di gestione privacy. L'elenco dei soggetti nominati responsabili esterni del trattamento dati e delle funzioni esternalizzate è riportato sul "Mansionario", allegato al presente documento.

7. Allegati
Analisi dei rischi
Disciplinare interno per l'uso della posta elettronica e di internet
Elenco dei trattamenti
Elenco Hardware
Elenco misure adottate
Mansionario
Piano di formazione
Piano di miglioramento
Report segnalazioni
Scheda Backup

Revisione del documento: 100 , Data di revisione: 31/03/2017

Il Dirigente Scolastico
Prof. Anselmo Grotti