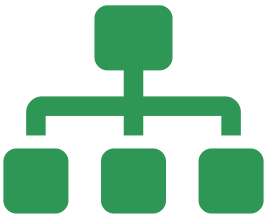
Istituto Comprensivo "Aldo Moro" di Campagna Lupia



Registro dei trattamenti

Titolare del trattamento

Nome: Istituto Comprensivo "Aldo Moro" di Campagna Lupia
Email: veic816009@istruzione.it
Pec: veic816009@pec.istruzione.it
Telefono: 041460046

Responsabile della protezione dati

Nome: Marco Babolin
Email: dpo@robyone.net
Pec: dpo.robyone@ronepec.it
Telefono: 0490998416

Via Maria Montessori, 7 - 30010 Campagna Lupia (VE)
Tel.: 041460046 - Mail: veic816009@istruzione.it - PEC: veic816009@pec.istruzione.it

Indice dei contenuti

Via Maria Montessori, 7 - 30010 Campagna Lupia (VE)
Tel.: 041460046 - Mail: veic816009@istruzione.it - PEC: veic816009@pec.istruzione.it

1 Acquisti

Finalità

Pubblicità, Gestione dei fornitori, Monitoraggio degli adempimenti contrattuali, Adempimento di obblighi fiscali e contabili

Categorie di interessati

Fornitori Esterni / Professionisti, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Professionista, Azienda di servizi

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Attività economiche, commerciali, finanziarie e assicurative, Indirizzo e-mail e numero cellulare, Informazioni di carattere giudiziario (GDPR 679/2016, art. 10), Beni, proprietà, possesso, compresi dati relativi al patrimonio immobiliare

Categorie di destinatari

Amministrativo generico, Amministratore di sistema, Delegato - Direttore dei Servizi Generali Amministrativi, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Banche e istituti di credito, Altre amministrazioni Pubbliche, Diffusione al pubblico

Termini ultimi previsti per la cancellazione

10 anni dopo il termine del contratto

2 Contabilità e Patrimonio

Finalità

Gestione del patrimonio mobiliare e immobiliare, Gestione dei fornitori, Trattamento giuridico ed economico del personale, Monitoraggio degli adempimenti contrattuali, Adempimento di obblighi fiscali e contabili, Adempimenti connessi al versamento delle quote di iscrizioni a sindacati o all'esercizio di diritti sindacali

Categorie di interessati

Dipendenti, Fornitori Esterni / Professionisti, Familiari

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Attività economiche, commerciali, finanziarie e assicurative, Beni, proprietà, possesso, compresi dati relativi al patrimonio immobiliare, Coordinate bancarie

Categorie di destinatari

Amministrativo generico, Amministratore di sistema, Amministrativo personale, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Enti locali, Banche e istituti di credito, Altre amministrazioni Pubbliche, Diffusione al pubblico

Termini ultimi previsti per la cancellazione

Come da normativa vigente

3 Gestione Alunni

Finalità

Istruzione e assistenza scolastica

Via Maria Montessori, 7 - 30010 Campagna Lupia (VE)
Tel.: 041460046 - Mail: veic816009@istruzione.it - PEC: veic816009@pec.istruzione.it

Categorie di interessati

Alunno, Familiari

Categorie di dati personali

Nominativo, indirizzo o altri elementi di identificazione personale, Stato di salute – patologie attuali, Stato di salute – terapie in corso, Stato di salute - altro, Codice fiscale ed altri numeri di identificazione personale, Carte sanitarie, Dati relativi alla famiglia o a situazioni personali, Dati sul comportamento, profili di utenti, consumatori, contribuenti, ecc., Indirizzo e-mail e numero cellulare, Informazioni di carattere giudiziario (GDPR 679/2016, art. 10), Istruzione

Categorie di destinatari

Collaboratore scolastico, Amministratore di sistema, Docente, Amministrativo didattica, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Enti locali, Istituti, scuole e università, Enti previdenziali ed assistenziali, Altre amministrazioni Pubbliche, Imprese di assicurazione, Associazioni e cooperative

Termini ultimi previsti per la cancellazione

Come da normativa vigente

4 Gestione Immagini e Video

Finalità

Attività promozionali

Categorie di interessati

Alunno

Categorie di dati personali

Immagini, Fotografie

Categorie di destinatari

Dipendenti, Amministratore di sistema, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Familiari

Termini ultimi previsti per la cancellazione

Per un anno dopo il termine del contratto per le foto individuali, per le foto di gruppo illimitata

5 Gestione Risorse Umane

Finalità

Trattamento giuridico ed economico del personale, Reclutamento, selezione, valutazione e monitoraggio del personale, Monitoraggio degli adempimenti contrattuali, Igiene e sicurezza del lavoro, Gestione del personale, Adempimento di obblighi fiscali e contabili, Adempimenti connessi al versamento delle quote di iscrizioni a sindacati o all'esercizio di diritti sindacali

Categorie di interessati

Dipendenti

Categorie di dati personali

Codice fiscale ed altri numeri di identificazione personale, Nominativo, indirizzo o altri elementi di identificazione personale, Lavoro (occupazione attuale, precedente, curriculum, certificati di qualità professionali, ecc.), Istruzione, Stato di salute - altro, Attività economiche, commerciali, finanziarie e assicurative, Dati sul comportamento, profili di utenti, consumatori, contribuenti, ecc., Dati relativi alla famiglia o a situazioni personali, Idoneità al lavoro, Carte sanitarie, Iscrizione a sindacato, Indirizzo e-mail e numero cellulare, Informazioni di carattere giudiziario (GDPR 679/2016, art. 10)

Categorie di destinatari

Amministratore di sistema, Amministrativo personale, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Banche e istituti di credito, Intermediari finanziari, Istituti, scuole e università, Enti previdenziali ed assistenziali, Altre amministrazioni Pubbliche, Organizzazioni sindacali e patronati, Imprese di assicurazione, Diffusione al pubblico

Termini ultimi previsti per la cancellazione

Illimitata

6 Inserimento Alunni

Finalità

Istruzione e assistenza scolastica

Categorie di interessati

Alunno, Familiari

Categorie di dati personali

Nominativo, indirizzo o altri elementi di identificazione personale, Istruzione, Codice fiscale ed altri numeri di identificazione personale, Dati relativi alla famiglia o a situazioni personali

Categorie di destinatari

Amministratore di sistema, Docente, Amministrativo didattica, Azienda fornitrice programmi applicativi, Amministratore di Sistema, Altre amministrazioni Pubbliche, Imprese di assicurazione

Termini ultimi previsti per la cancellazione

Come da normativa vigente

7 Descrizione generale delle misure di sicurezza tecniche e organizzative

- **Accordi di riservatezza o di non divulgazione**
  I requisiti per gli accordi di riservatezza o di non divulgazione che riflettono le necessità dell'organizzazione per la protezione delle informazioni devono essere identificati, riesaminati periodicamente e documentati
- **Apparecchiature incustodite degli utenti**
  Gli utenti devono assicurare che le apparecchiature incustodite siano appropriatamente protette
- **Backup delle informazioni**
  Devono essere effettuate copie di backup delle informazioni, del software e delle immagini dei sistemi e quindi sottoposte a test periodici secondo una politica di backup concordata
- **Cessazione o variazione delle responsabilità durante il rapporto di lavoro**
  Le responsabilità e i doveri relativi alla sicurezza delle informazioni che rimangono validi dopo la cessazione o la variazione del rapporto di lavoro devono essere definiti, comunicati al personale o al collaboratore e resi effettivi

Via Maria Montessori, 7 - 30010 Campagna Lupia (VE)
Tel.: 041460046 - Mail: veic816009@istruzione.it - PEC: veic816009@pec.istruzione.it

- **Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni**
  Tutto il personale dell'organizzazione e, quando pertinente, il collaboratore, devono ricevere un'adeguata sensibilizzazione, istruzione, formazione e addestramento e aggiornamenti periodici sulle politiche e procedure organizzative, in modo pertinente alla loro attività lavorativa
- **Controlli contro il malware**
  Devono essere attuati controlli di individuazione, di prevenzione e di ripristino relativamente al malware, congiuntamente ad un'appropriata consapevolezza degli utenti
- **Controlli di accesso fisico**
  Le aree di sicurezza devono essere protette da appropriati controlli per l'ingresso atti ad assicurare che solo il personale autorizzato abbia il permesso di accedervi
- **Controlli di rete**
  Le reti devono essere gestite e controllate per proteggere le informazioni nei sistemi e nelle applicazioni. Firewall, VLAN, eccetera.
- **Dismissione dei supporti**
  La dismissione dei supporti non più necessari deve avvenire in modo sicuro, attraverso l'utilizzo di procedure formali. Questo controllo è per i documenti e le memorie come chiavi USB, CD e DVD, nastri (per i dispositivi, vedere A.11.02.07). Include anche la gestione dei documenti in bozza. Include anche la restituzione o distruzione dei dati al termine delle operazioni.
- **Dismissione sicura o riutilizzo delle apparecchiature**
  Tutte le apparecchiature contenenti supporti di memorizzazione devono essere controllate per assicurare che ogni dato critico od il software concesso in licenza sia rimosso o sovrascritto in modo sicuro prima della dismissione o del riutilizzo
- **Disponibilità delle strutture per l'elaborazione delle informazioni**
  Le strutture per l'elaborazione delle informazioni devono essere realizzate con una ridondanza sufficiente a soddisfare i requisiti di disponibilità
- **Disposizione delle apparecchiature e loro protezione**
  Le apparecchiature devono essere disposte e protette al fine di ridurre i rischi derivanti dalle minacce e dai pericoli ambientali, oltre alle occasioni di accesso non autorizzato
- **Gestione dei diritti di accesso privilegiato**
  L'assegnazione e l'uso di diritti di accesso privilegiato devono essere limitati e controllati
- **Gestione dei supporti rimovibili**
  Devono essere sviluppate procedure per il trattamento dei supporti rimovibili in base allo schema di classificazione adottato dall'organizzazione
- **Gestione delle vulnerabilità tecniche**
  Le informazioni sulle vulnerabilità tecniche dei sistemi informativi utilizzati devono essere ottenute in modo tempestivo, l'esposizione a tali vulnerabilità deve essere valutata e appropriate misure devono essere intraprese per affrontare i rischi relativi. Patching
- **Infrastrutture di supporto**
  Le apparecchiature devono essere protette da malfunzionamenti alla rete elettrica di alimentazione e da altri disservizi causati da malfunzionamenti dei servizi ausiliari
- **Inventario degli asset**
  Tutti gli asset associati alle informazioni e alle strutture di elaborazione delle informazioni devono essere identificati; un inventario di questi asset deve essere compilato e mantenuto aggiornato
- **Limitazione dell'accesso alle informazioni**
  L'accesso a informazioni e funzioni di sistemi applicativi deve essere limitato secondo le politiche di controllo degli accessi
- **Limitazioni all'installazione del software**
  Devono essere stabilite e attuate regole per il governo dell'installazione del software da parte degli utenti
- **Log di amministratori e operatori**
  Le attività degli amministratori e degli operatori di sistema devono essere sottoposte a log, e questi devono essere protetti e riesaminati periodicamente
- **Manutenzione delle apparecchiature**
  Le apparecchiature devono essere correttamente mantenute per assicurare la loro continua disponibilità e integrità
- **Messaggistica elettronica**
  Le informazioni trasmesse attraverso messaggistica elettronica devono essere protette in modo appropriato

Via Maria Montessori, 7 - 30010 Campagna Lupia (VE)
Tel.: 041460046 - Mail: veic816009@istruzione.it - PEC: veic816009@pec.istruzione.it

- **Politica di controllo degli accessi**
  Una politica di controllo degli accessi deve essere definita, documentata ed aggiornata sulla base dei requisiti di business e di sicurezza delle informazioni
- **Politica per la sicurezza delle informazioni nei rapporti con i fornitori**
  I requisiti di sicurezza delle informazioni per mitigare i rischi associati all'accesso agli asset dell'organizzazione da parte dei fornitori devono essere concordati con i fornitori stessi e documentati
- **Politica sull'uso dei controlli crittografici**
  Deve essere sviluppata e attuata una politica sull'uso dei controlli crittografici per la protezione delle informazioni. Per i dati sui server e sui database, per i pc e i dispositivi portatili (p.e. smartphone e tablet), per le memorie rimovibili (p.e. chiavi USB), per la trasmissione.
- **Politiche per la sicurezza delle informazioni**
  Un insieme di politiche per la sicurezza delle informazioni deve essere definito, approvato dalla direzione, pubblicato e comunicato al personale e alle parti esterne pertinenti
- **Processo disciplinare**
  Deve essere istituito un processo disciplinare, formale e comunicato, per intraprendere provvedimenti nei confronti del personale che ha commesso una violazione della sicurezza delle informazioni
- **Protezione contro minacce esterne ed ambientali**
  Deve essere progettata e applicata un'adeguata protezione fisica da calamità naturali, attacchi malevoli o accidenti
- **Rimozione o adattamento dei diritti di accesso**
  I diritti di accesso di tutto il personale e degli utenti di parti esterne a informazioni e strutture di elaborazione delle informazioni devono essere rimossi al momento della cessazione del rapporto di lavoro, del contratto o accordo, oppure adattate ad ogni variazione
- **Ruoli e responsabilità per la sicurezza delle informazioni**
  Tutte le responsabilità relative alla sicurezza delle informazioni dovrebbero essere definite e assegnate
- **Segregazione nelle reti**
  Nelle reti si devono segregare gruppi di servizi, di utenti e di sistemi informativi
- **Sicurezza dei cablaggi**
  I cavi per l'energia elettrica e le telecomunicazioni adibiti al trasporto di dati o a supporto di servizi informativi devono essere protetti da intercettazioni, interferenze o danneggiamenti
- **Sincronizzazione degli orologi**
  Gli orologi di tutti i sistemi pertinenti che elaborano informazioni all'interno di un'organizzazione o di un dominio di sicurezza devono essere sincronizzati rispetto a una singola sorgente temporale di riferimento
- **Sistema di gestione delle password**
  I sistemi di gestione delle password devono essere interattivi e devono assicurare password di qualità
- **Termini e condizioni di impiego**
  Gli accordi contrattuali con il personale e con i collaboratori devono specificare le responsabilità loro e dell'organizzazione relativamente alla sicurezza delle informazioni
- **Trattamento degli asset**
  Deve essere sviluppato e attuato un insieme di procedure per il trattamento degli asset in base allo schema di classificazione adottato dall'organizzazione
- **Utilizzo accettabile degli asset**
  Le regole per l'utilizzo accettabile delle informazioni e degli asset associati alle strutture di elaborazione delle informazioni devono essere identificate, documentate e attuate. Regole al personale anche relative a: uso dei dispositivi portatili, BYOD, scrivania pulita, schermo pulito, trasporto (p.e. dei documenti cartacei), blocco dei pc quando non usati, eccetera.